The US-CERT Cyber Security Bulletin provides a summary of new and updated vulnerabilities, exploits, trends, and malicious code that have recently been openly reported. Information in the Cyber Security Bulletin is a compilation of open source and US-CERT vulnerability information. As such, the Cyber Security Bulletin includes information published by sources outside of US-CERT and *should* ***not*** *be considered the result of US-CERT analysis or as an official report of US-CERT*. Although this information does reflect open source reports, it is not an official description and should be used for informational purposes only. The intention of the Cyber Security Bulletin is to serve as a comprehensive directory of pertinent vulnerability reports, providing brief summaries and additional sources for further investigation.

# Vulnerabilities

The tables below summarize vulnerabilities that have been reported by various open source organizations or presented in newsgroups and on web sites. Items in bold designate updates that have been made to past entries. Entries are grouped by the operating system on which the reported software operates, and vulnerabilities which affect both Windows and Unix/ Linux Operating Systems are included in the Multiple Operating Systems table. *Note*, entries in each table are not necessarily vulnerabilities *in* that operating system, but vulnerabilities in software which operate on some version of that operating system.

Entries may contain additional US-CERT sponsored information, including Common Vulnerabilities and Exposures (CVE) numbers, National Vulnerability Database (NVD) links, Common Vulnerability Scoring System (CVSS) values, Open Vulnerability and Assessment Language (OVAL) definitions, or links to US-CERT Vulnerability Notes. Metrics, values, and information included in the Cyber Security Bulletin which has been provided by other US-CERT sponsored programs, is prepared, managed, and contributed by those respective programs. CVSS values are managed and provided by the US-CERT/ NIST National Vulnerability Database. Links are also provided to patches and workarounds that have been provided by the product's vendor.

**The Risk levels are defined below:**

**High** - Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

**Medium** - Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.

**Low** - Vulnerabilities will be labeled "Low" severity if they have a CVSS base score of 0.0-3.9.

*Note that scores provided prior to 11/9/2005 are approximated from only partially available CVSS metric data. Such scores are marked as "Approximated" within NVD. In particular, the following CVSS metrics are only partially available for these vulnerabilities and NVD assumes certain values based on an approximation algorithm: AccessComplexity, Authentication, ConfImpact of 'partial', IntegImpact of 'partial', AvailImpact of 'partial', and the impact biases.*

# Windows Operating Systems Only

| Vendor & Software Name | Description | Common Name | CVSS | Resources |
|---|---|---|---|---|
| Aquifer CMS | A vulnerability has been reported in Aquifer CMS that could let remote malicious users conduct Cross-Site Scripting.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | Aquifer CMS Cross Site Scripting<br>CVE-2006-0122 | 2.3 | Security Focus, ID: 16162, January 6, 2006 |
| Blue Coat Systems<br>WinProxy 6.0 | Multiple vulnerabilities have been reported in WinProxy that could let remote malicious users cause a Denial of Service.<br>Blue Coat Systems<br>There is no exploit code required. | Blue Coat WinProxy Multiple Vulnerabilities<br>CVE-2005-3187<br>CVE-2005-3654<br>CVE-2005-4085 | 2.3 (CVE-2005-3187)<br>9 (CVE-2005-3654)<br>8 (CVE-2005-4085) | Secunia, Advisory: SA18288, January 6, 2006 |
| Microsoft<br>Excel 95, 97, 2000, 2002 | A vulnerability has been reported in Excel that could let remote malicious users execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>Currently we are not aware of any exploits for this vulnerability. | Microsoft Excel Arbitrary Code Execution | Not available | Security Focus, ID: 16181, January 9, 2006 |
| Microsoft<br>Exchange 5.0 SP2, 5.5 SP4, 2000, Outlook | A buffer overflow vulnerability has been reported in Outlook and Exchange that could let remote malicious users execute arbitrary code.<br>Microsoft<br>Currently we are not aware of any exploits for this vulnerability. | Microsoft Outlook & Exchange Arbitrary Code Execution<br>CVE-2006-0002 | 7 | Microsoft, Security Bulletin MS06-003, January 10, 2006<br>US-CERT VU#252146 |
| Microsoft<br>Visual Studio Visual C# 2005 Express Edition | A vulnerability has been reported in Visual Studio that could let remote malicious users execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>Currently we are not aware of any exploits for this vulnerability. | Microsoft Visual Studio Arbitrary Code Execution<br>CVE-2006-0187 | 4.5 | Secunia, Advisory: SA18409, January 11, 2006 |
| Microsoft<br>Windows 98, 2000 SP4, XP SP2, 2003 | A buffer overflow vulnerability has been reported in Windows that could let remote malicious users execute arbitrary code.<br>Windows<br>Avaya<br>Currently we are not aware of any exploits for this vulnerability. | Microsoft Windows Arbitrary Code Execution<br>CVE-2006-0010 | 7 | Microsoft, Security Bulletin MS06-002, January 10, 2006<br>Avaya, Number: ASA-2006-004, January 10, 2006<br>US-CERT VU#915930 |
| Microsoft<br>Windows Meta File (WMF) Graphics Rendering Engine | A vulnerability has been reported in Windows Meta File (WMF) Graphics Rendering Engine could let remote malicious users execute arbitrary code.<br>Microsoft<br>**Avaya**<br>Currently we are not aware of any exploits for this vulnerability. | Microsoft Windows WMF Rendering Engine Arbitrary Code Execution<br>CVE-2005-4560 | 8 | Microsoft, Security Advisory 912840, December 28, 2005<br>US-CERT VU#181038<br>**Avaya, Number: ASA-2006-001, January 5, 2006** |
| NetSarang<br>Xlpd 2.1 | A vulnerability has been reported in Xlpd that could let remote malicious users cause a Denial of Service.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | Xlpd Denial of Service<br>CVE-2006-0148 | 2.3 | Security Tracker, Alert ID: 1015444, January 6, 2006 |

|  |  |  |  |  |
|---|---|---|---|---|
| PD9 Software<br>MegaBBS 2.0, 2.1 | A vulnerability has been reported in MegaBBS that could let remote malicious users disclose information.<br>PD9 Software<br>There is no exploit code required. | MegaBBS Information Disclosure<br>CVE-2006-0139 | 2.3 | Security Focus, ID: 16168, January 9, 2006 |
| PHP 4.3.10, 4.4.0, and 4.4.1 for Windows | A buffer overflow vulnerability has been reported in PHP, mysql_connect, that could let malicious users execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>An exploit, phpflaw.obj, has been published. | PHP Arbitrary Code Execution<br>CVE-2006-0097 | 7 | Security Focus, ID: 16145, January 5, 2006 |
| Rockliffe<br>MailSite Email Server 6.1.22 | A vulnerability has been reported in MailSite that could let remote malicious users disclose information.<br>Rockliffe<br>Currently we are not aware of any exploits for this vulnerability. | MailSite Information Disclosure<br>CVE-2006-0127 | 1.4 | Secunia, Advisory: SA18318, January 5, 2006 |
| Symantec<br>Norton SystemWorks 2005, 2006 | A vulnerability has been reported in Norton SystemWorks that could let local malicious users bypass security restrictions.<br>Patch reportedly available via LiveUpdate.<br>Currently we are not aware of any exploits for this vulnerability. | Symantec Norton SystemWorks Security Bypassing<br>CVE-2006-0166 | Not available | Secunia, Advisory: SA18402, January 11, 2006 |
| WebWiz Forum 6.34 | A vulnerability has been reported in WebWiz Forum that could let remote malicious users conduct Cross-Site Scripting.<br>WebWiz<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | WebWiz Forums Cross Site Scripting<br>CVE-2006-0175 | Not available | Security Focus, ID: 16196, January 10, 2006 |

[back to top]

## UNIX / Linux Operating Systems Only

| Vendor & Software Name | Description | Common Name | CVSS | Resources |
|---|---|---|---|---|
| Bogofilter Email Filter<br>Bogofilter Email Filter 0.96.2, 0.95.2, 0.94.14, 0.94.12, 0.93.5 | Several buffer overflow vulnerabilities have been reported: a vulnerability was reported in bogofilter and bogolexer when character set conversion is performed on invalid input sequences, which could let a remote malicious user cause a Denial of Service; and a vulnerability was reported in bogofilter and bogolexer when processing input that contains overly long words, which could let a remote malicious user cause a Denial of Service.<br>Upgrade available<br>Ubuntu<br>There is no exploit code required. | Bogofilter Multiple Remote Buffer Overflows<br>CVE-2005-4591<br>CVE-2005-4592 | 9<br>(CVE-2005-4591)<br>9<br>(CVE-2005-4592) | Bogofilter Security Advisories, bogofilter-SA-2005-01 & 02, January 2, 2006<br>Ubuntu Security Notice, USN-240-1, January 11, 2006 |
| Clam Anti-Virus<br>ClamAV 0.80 - 0.87.1, 0.75.1, 0.70, 0.68, 0.67, 0.65, 0.60, 0.51-0.54 | A buffer overflow vulnerability has been reported when attempting to handle compressed UPX files due to an unspecified boundary error in "libclamav/upx.c, which could let a remote malicious user execute arbitrary code.<br>ClamAV<br>Currently we are not aware of any exploits for this vulnerability. | ClamAV UPX File Handling<br>CVE-2006-0162 | 8 | Secunia Advisory: SA18379, January 10, 2006 |

| | | | | |
|---|---|---|---|---|
| Easy Software Products<br>CUPS prior to 1.1.21rc1 | A vulnerability has been reported in incoming print jobs due to a failure to properly apply ACLs (Access Control List), which could let a remote malicious user bypass ACLs.<br>Cups<br>RedHat<br>Fedora<br>Ubuntu<br>**Conectiva**<br>There is no exploit code required. | Easy Software Products CUPS Access Control List Bypass<br>CVE-2004-2154 | 7 | Security Tracker Alert ID: 1014482, July 14, 2005<br>RedHat Security Advisory, RHSA-2005: 571-06, July 14, 2005<br>Fedora Legacy Update Advisory, FLSA:163274, September 14, 2005<br>Ubuntu Security Notice, USN-185-1, September 20, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1055, January 2, 2006** |
| Ethereal Group<br>Ethereal 0.8, 0.8.13-0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.8 | Multiple vulnerabilities exist: remote Denial of Service vulnerabilities exist in the COPS, DLSw, DNP, Gnutella, and MMSE dissectors; and a buffer overflow vulnerability exists in the X11 dissector, which could let a remote malicious user execute arbitrary code.<br>Ethereal<br>Debian<br>Gentoo<br>SuSE:<br>SGI<br>ALT Linux<br>Conectiva<br>**FedoraLegacy**<br>Currently we are not aware of any exploits for these vulnerabilities. | Ethereal Multiple Dissector Vulnerabilities<br>CVE-2005-0006<br>CVE-2005-0007<br>CVE-2005-0008<br>CVE-2005-0009<br>CVE-2005-0010<br>CVE-2005-0084 | 3.3 (CVE-2005-0006)<br>3.3 (CVE-2005-0007)<br>3.3 (CVE-2005-0008)<br>3.3 (CVE-2005-0009)<br>3.3 (CVE-2005-0010)<br>7 (CVE-2005-0084) | Security Tracker Alert, 1012962, January 21, 2005<br>SGI Security Advisory, 20050202-01-U, February 9, 2005<br>Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005<br>ALTLinux Security Advisory, March 29, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |
| FreeBSD<br>FreeBSD 6.0 -STABLE, 6.0 -RELEASE | A remote Denial of Service vulnerability has been reported due to an error in the "ipfw" module when handling IP fragments.<br>FreeBSD<br>There is no exploit code required; however, exploit details, rt-sa-2005-15.txt, have been published. | FreeBSD IPFW IP Fragment Remote Denial of Service<br>CVE-2006-0054 | 2.3 | FreeBSD Security Advisory, FreeBSD-SA-06:04.ipfw, January 11, 2006 |
| FreeBSD<br>FreeBSD 4.x<br>FreeBSD 5.x<br>FreeBSD 6.x | A vulnerability has been reported in the 'EE' editor when executing a spell check operation due to the insecure creation of temporary files, which could let a malicious user obtain elevated privileges.<br>FreeBSD<br>There is no exploit code required. | FreeBSD Insecure Temporary File Creation<br>CVE-2006-0055 | 1.6 | FreeBSD Security Advisory, FreeBSD-SA-06:02.ee, January 11, 2006 |

|  |  |  |  |  |
|---|---|---|---|---|
| GNU<br>cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6 | A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions.<br>Trustix<br>Mandriva<br>RedHat<br>SGI<br>SCO<br>Avaya<br>Conectiva<br>Ubuntu<br>Debian<br>RedHat<br>SCO<br>**FreeBSD**<br>There is no exploit code required. | CPIO CHMod File Permission Modification<br>CVE-2005-1111 | 4.9 | Bugtraq, 395703, April 13, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005<br>Mandriva Linux Security Update Advisory, MDKSA2005: 116, July 12, 2005<br>RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005<br>SGI Security Advisory, 20050802-01-U, August 15, 2005<br>SCO Security Advisory, SCOSA-2005.32, August 18, 2005<br>Avaya Security Advisory, ASA-2005-191, September 6, 2005<br>Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005<br>Ubuntu Security Notice, USN-189-1, September 29, 2005<br>Debian Security Advisory, DSA 846-1, October 7, 2005<br>RedHat Security Advisory, RHSA-2005:806-8, November 10, 2005<br>SCO Security Advisory, SCOSA-2006.2, January 3, 2006<br>**FreeBSD Security Advisory, FreeBSD-SA-06:03.cpio, January 11, 2006** |
| GNU<br>cpio 2.6 | A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information.<br>Gentoo<br>Trustix/<br>Mandriva<br>SCO<br>Avaya<br>Conectiva<br>Ubuntu<br>Debian<br>SCO<br>**FreeBSD**<br>A Proof of Concept exploit has been published. | CPIO Directory Traversal<br>CVE-2005-1229 | 4.9 | Bugtraq, 396429, April 20, 2005<br>Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005<br>Mandriva Linux Security Update Advisory, MDKSA2005: 116, July 12, 2005<br>SCO Security Advisory, SCOSA-2005.32, August 18, 2005<br>Avaya Security Advisory, ASA-2005-191, September 6, 2005<br>Conectiva Linux Announcement, CLSA-2005:1002, September 13, 2005<br>Ubuntu Security Notice, USN-189-1, September 29, 2005<br>Debian Security Advisory, DSA 846-1, October 7, 2005<br>SCO Security Advisory, SCOSA-2006.2, January 3, 2006<br>**FreeBSD Security Advisory, FreeBSD-SA-06:03.cpio,** |

| | | | | |
|---|---|---|---|---|
| | | | | **January 11, 2006** |
| GNU<br>cpio 2.6, 2.5 | A Denial of Service vulnerability has been reported due to a buffer overflow when cpio attempts to create an archive containing extremely large files.<br>Mandriva<br>Ubuntu<br>**FreeBSD**<br>Currently we are not aware of any exploits for this vulnerability. | CPIO File Size Stack Denial of Service<br>CVE-2005-4268 | 4.9 | Mandriva Linux Security Advisory MDKSA-2005:237, December 23, 2005<br>Ubuntu Security Notice, USN-234-1, January 02, 2006<br>**FreeBSD Security Advisory, FreeBSD-SA-06:03.cpio, January 11, 2006** |
| GNU<br>Texinfo 4.7 | A vulnerability has been reported in 'textindex.c' due to insecure creation of temporary files by the 'sort_offline()' function, which could let a malicious user create/ overwrite arbitrary files.<br>Gentoo<br>Mandriva<br>Ubuntu<br>SUSE<br>Trustix<br>**FreeBSD**<br>There is no exploit code required. | GNU Texinfo Insecure Temporary File Creation<br>CVE-2005-3011 | 2.3 | Security Focus, Bugtraq ID: 14854, September 15, 2005<br>Gentoo Linux Security Advisory, GLSA 200510-04, October 5, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:175, October 6, 2005<br>Ubuntu Security Notice, USN-194-1, October 06, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005<br>**FreeBSD Security Advisory, FreeBSD-SA-06:01.texindex, January 11, 2006** |
| IPsec-Tools<br>IPsec-Tools0.6-0.6.2, 0.5-0.5.2 | A remote Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions when in 'AGGRESSIVE' mode.<br>IpsecTools<br>Ubuntu<br>Gentoo<br>SUSE<br>**Conectiva**<br>Vulnerability can be reproduced with the PROTOS IPSec Test Suite. | IPsec-Tools ISAKMP IKE Remote Denial of Service<br>CVE-2005-3732 | 5 | Security Focus, Bugtraq ID: 15523, November 22, 2005<br>Ubuntu Security Notice, USN-221-1, December 01, 2005<br>Gentoo Linux Security Advisory, GLSA 200512-04, December 12, 2005<br>SUSE Security Announcement, SUSE-SA:2005:070, December 20, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1058, January 2, 2006** |
| Multiple Vendors<br>Xpdf 3.0 pl2 & pl3, 3.0 1, 3.00, 2.0-2.03, 1.0 0, 1.0 0a, 0.90-0.93; RedHat Fedora Core4, Core3, Enterprise Linux WS 4, WS 3, WS 2.1 IA64, WS 2.1, ES 4, ES 3, ES 2.1 IA64, 2.1, Enterprise Linux AS 4, AS 3, 2.1 IA64, 2.1, Desktop 4.0, 3.0, Advanced Workstation for the Itanium Processor 2.1 IA64, 2.1; teTeX 2.0.1, 2.0; Poppler poppler 0.4.2;<br>KDE kpdf 0.5, KOffice 1.4.2 ;<br>PDFTOHTML DFTOHTML 0.36 | Multiple vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported in the 'DCTStream::read BaselineSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'DCTStream::read ProgressiveSOF()' function in 'xpdf/Stream.cc' when copying data from a PDF file, which could let a remote malicious user potentially execute arbitrary code; a buffer overflow vulnerability was reported in the 'StreamPredictor:: StreamPredictor()' function in 'xpdf/Stream.cc' when using the 'numComps' value to calculate the memory size, which could let a remote malicious user potentially execute arbitrary code; and a vulnerability was reported in the 'JPXStream: :readCodestream()' function in 'xpdf/JPXStream.cc' when using the 'nXTiles' and 'nYTiles' values from a PDF file to copy data from the file into allocated memory, which could let a remote malicious user potentially execute arbitrary code.<br>Patches available<br>Fedora | Xpdf Buffer Overflows<br>CVE-2005-3191<br>CVE-2005-3192<br>CVE-2005-3193 | 4.8<br>(CVE-2005-3191)<br>7<br>(CVE-2005-3192)<br>4.8<br>(CVE-2005-3193) | iDefense Security Advisory, December 5, 2005<br>Fedora Update Notifications, FEDORA-2005-1121 & 1122, December 6, 2005<br>RedHat Security Advisory, RHSA-2005:840-5, December 6, 2005<br>KDE Security Advisory, advisory-20051207-1, December 7, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005<br>Ubuntu Security Notice, USN-227-1, December 12, 2005<br>Gentoo Linux Security Advisory, GLSA 200512-08, December 16, 2005<br>RedHat Security Advisories, RHSA-2005:868-4, |

| | | | | |
|---|---|---|---|---|
| | RedHat<br>KDE<br>SUSE<br>Ubuntu<br>Gentoo<br>RedHat<br>RedHat<br>RedHat<br>**Mandriva**<br>**Debian**<br>Currently we are not aware of any exploits for these vulnerabilities. | | | RHSA-2005:867-5 & RHSA-2005:878-4, December 20, 2005<br>**Mandriva Linux Security Advisories MDKSA-2006:003-003-006, January 6, 2006**<br>**Debian Security Advisory, DSA-936-1, January 11, 2006** |
| Multiple Vendors<br>Glyph and Cog Xpdf 3.0, pl2 & pl3;<br>Ubuntu Linux 5.0 4 powerpc, i386, amd64;<br>RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;<br>KDE 3.4.1, 3.4, 3.3.1, 3.3.2;<br>GNOME GPdf 2.8.3, 2.1 | A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files.<br>RedHat<br>RedHat<br>RedHat<br>Ubuntu<br>KDE<br>Mandriva<br>SGI<br>Gentoo<br>Fedora<br>Debian<br>Trustix<br>TurboLinux<br>Conectiva<br>Mandriva<br>SCO<br>**Debian**<br>Currently we are not aware of any exploits for this vulnerability. | XPDF Loca Table Verification Remote Denial of Service<br>CVE-2005-2097 | 2.3 | RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005<br>Ubuntu Security Notice, USN-163-1, August 09, 2005<br>KDE Security Advisory, 20050809-1, August 9, 2005<br>Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005<br>SGI Security Advisory, 20050802-01-U, August 15, 2005<br>Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005<br>Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005<br>Debian Security Advisory, DSA 780-1, August 22, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005<br>Turbolinux Security Advisory, TLSA-2005-88, September 5, 2005<br>Conectiva Linux Announcement, CLSA-2005:1010, September 13, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:138-1, September 19, 2005<br>SCO Security Advisory, SCOSA-2005.42, October 20, 2005<br>**Debian Security Advisory, DSA-936-1, January 11, 2006** |

| | | | | |
|---|---|---|---|---|
| Multiple Vendors<br>ht://Dig Group ht://Dig 3.1.5 -8, 3.1.5 -7, 3.1.5, 3.1.6, 3.2 .0, 3.2 0b2-0b6; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, 9.0 x86_64, 9.1, 9.2 | A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'config' parameter, which could let a remote malicious user execute arbitrary HTML and script code.<br>SuSE<br>Debian<br>Gentoo<br>Mandrake<br>Fedora<br>SCO<br>**FedoraLegacy**<br>Proof of Concept exploit has been published. | ht://Dig Cross-Site Scripting<br>CVE-2005-0085 | 7 | SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005<br>Debian Security Advisory, DSA 680-1, February 14, 2005<br>Gentoo Linux Security Advisory, GLSA 200502-16, February 14, 2005<br>Mandrakelinux Security Update Advisory, MDKSA-2005:063, March 31, 2005<br>Fedora Update Notification, FEDORA-2005-367, April 19, 2005<br>SCO Security Advisory, SCOSA-2005.46, November 2, 2005<br>**Fedora Legacy Update Advisory, FLSA:152907, January 9, 2006** |
| Multiple Vendors<br>Hylafax 4.2-4.2.3;<br>Gentoo Linux | Several vulnerabilities have been reported: a vulnerability was reported in 'hfaxd' when compiled with PAM support disabled, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported due to insufficient sanitization of the 'notify' script, which could let a remote malicious user execute arbitrary commands; and a vulnerability was reported in the 'faxrcvd' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary commands.<br>Hylafax<br>Gentoo<br>There is no exploit code required; however, Proof of Concept exploits have been published. | HylaFAX Authentication Bypass & Arbitrary Command Execution<br>CVE-2005-3538<br>CVE-2005-3539 | 7<br>(CVE-2005-3538)<br>8<br>(CVE-2005-3539) | Secunia Advisory: SA18314, January 6, 2006<br>Gentoo Linux Security Advisory GLSA 200601-03, January 6, 2006 |
| Multiple Vendors<br>Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6 | A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges.<br>Perl<br>Ubuntu<br>Gentoo<br>Debian<br>TurboLinux<br>Mandrake<br>HP<br>Fedora<br>Avaya<br>RedHat<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Perl 'rmtree()' Function Elevated Privileges<br>CVE-2005-0448 | 2.3 | Ubuntu Security Notice, USN-94-1 March 09, 2005<br>Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005<br>Debian Security Advisory, DSA 696-1 , March 22, 2005<br>Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005<br>HP Security Bulletin, HPSBUX01208, June 16, 2005<br>Secunia, Advisory: SA16193, July 25, 2005<br>Avaya Security Advisory, ASA-2005-196, September 13, 2005<br>RedHat Security Advisory, RHSA-2005:674-10, October 5, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1056, January 2, 2006** |
| Multiple Vendors<br>NetBSD 2.1, 2.0-2.0.3, 1.6-1.6.2, NetBSD Current<br>Linux kernel 2.6-2.6.15 -rc3 | A vulnerability has been reported because the system clock can be set to an arbitrary value, which could let malicious user bypass security restrictions.<br>NetBSD | BSD SecureLevel Time Setting Security Restriction Bypass | 1.6 | NetBSD Security Advisory, NetBSD-SA2006-002, January 9, 2006 |

| | | | | |
|---|---|---|---|---|
| | There is no exploit code required. | CVE-2005-4352 | | |
| Multiple Vendors<br>SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12 | A remote Denial of Service vulnerability has been reported in the NFSACL protocol when handling when handling XDR data.<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel NFSACL Protocol XDR Data Remote Denial of<br>CVE-2005-2500 | 8 | Security Focus, 14468, August 3, 2005<br>SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12 | A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code.<br>Linux Kernel<br>Ubuntu<br>SUSE<br>RedHat<br>Mandriva<br>RedHat<br>Mandriva<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel XFRM Array Index Buffer Overflow<br>CVE-2005-2456 | 2.3 | Security Focus, 14477, August 5, 2005<br>Ubuntu Security Notice, USN-169-1, August 19, 2005<br>SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005<br>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 200<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Trustix Secure Linux 3.0, 2.2, Secure Enterprise Linux 2.0, SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server for S/390 9.0, Linux Enterprise Server 9; 2.6-2.6.12 .4 | A Denial of Service vulnerability has been reported due to a failure to handle malformed compressed files.<br>Linux Kernel<br>Ubuntu<br>SUSE<br>Trustix<br>Mandriva<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel ZLib Null Pointer Dereference Denial of Service<br>CVE-2005-2459 | 3.3 | SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;<br>Todd Miller Sudo 1.6-1.6.8, 1.5.6-1.5.9 | A vulnerability has been reported in the 'PYTHONINSPECT' variable, which could let a malicious user bypass security restrictions and obtain elevated privileges.<br>Todd Miller Sudo<br>AppleWebSharing Update<br>Conectiva<br>Debian<br>EnGarde<br>Fedora | Sudo Python Environment Cleaning Security Bypass<br>CVE-2006-0151 | 7 | Security Focus, Bugtraq ID: 16184, January 9, 2006 |

FreeBSD

GratiSoft Sudo

Mandriva

OpenPKG

OpenBSD

RedHat

Slackware

SuSE

Trustix

TurboLinux

Ubuntu

Wirex

There is no exploit code required.

| | | | | |
|---|---|---|---|---|
| Multiple Vendors<br>zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux;<br>FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE;<br>Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3, 0.1-0.1.6 1, 0.0.1-0.0.6 | A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code.<br>Debian<br>FreeBSD<br>Gentoo<br>SUS<br>Ubuntu<br>Mandriva<br>OpenBSD<br>OpenPKG<br>RedHat<br>Trustix<br>Slackware<br>TurboLinux<br>Fedora<br>zsync<br>Apple<br>SCO<br>IPCop<br>Debian<br>Trolltech<br>FedoraLegacy<br>Gentoo<br>Debian<br>Trustix<br>Sun<br>Mandriva<br>Ubuntu<br>Ubuntu<br>**SCO**<br>Currently we are not aware of any exploits for this vulnerability. | Zlib Compression Library Buffer Overflow<br>CVE-2005-2096 | 8 | Debian Security Advisory DSA 740-1, July 6, 2005<br>FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005<br>Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005<br>SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005<br>Ubuntu Security Notice, USN-148-1, July 06, 2005<br>RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005<br>Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005<br>OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005<br>Slackware Security Advisory, SSA:2005-189-01, July 11, 2005<br>Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005<br>Fedora Update Notification, FEDORA-2005-565, July 13, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005<br>Security Focus, 14162, July 21, 2005<br>US-CERT VU#680620<br>Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005<br>SCO Security Advisory, SCOSA-2005.33, August 19, 2005<br>Security Focus, Bugtraq ID: 14162, August 26, 2005<br>Debian Security Advisory, DSA 797-1, September 1, 2005<br>Security Focus, Bugtraq ID: 14162, September 12, 2005<br>Fedora Legacy Update Advisory, FLSA:162680, September 14, 2005<br>Gentoo Linux Security Advisory, GLSA 200509-18, September 26, 2005 |

| | | | | |
|---|---|---|---|---|
| | | | | Debian Security Advisory, DSA 797-2, September 29, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005<br>Sun(sm) Alert Notification Sun Alert ID: 101989, October 14, 2005<br>Mandriva Linux Security Advisory MDKSA-2005:196, October 26, 2005<br>Ubuntu Security Notice, USN-151-3, October 28, 2005<br>Ubuntu Security Notice, USN-151-4, November 09, 2005<br>**SCO Security Advisory, SCOSA-2006.6, January 10, 2006** |
| Multiple Vendors<br>zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64,<br>4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k,<br>ia-64, ia-32,<br>hppa, arm,<br>alpha | A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input.<br>Zlib<br>Debian<br>Ubuntu<br>OpenBSD<br>Mandriva<br>Fedora<br>Slackware<br>FreeBSD<br>SUSE<br>Gentoo<br>Gentoo<br>Trustix<br>Conectiva<br>Apple<br>TurboLinux<br>SCO<br>Debian<br>Trolltech<br>FedoraLegacy<br>Debian<br>Mandriva<br>Ubuntu<br>Ubuntu<br>**SCO**<br>Currently we are not aware of any exploits for this vulnerability. | Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service<br>CVE-2005-1849 | 3.3 | Security Focus, Bugtraq ID 14340, July 21, 2005<br>Debian Security Advisory DSA 763-1, July 21, 2005<br>Ubuntu Security Notice, USN-151-1, July 21, 2005<br>OpenBSD, Release Errata 3.7, July 21, 2005<br>Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005<br>Secunia, Advisory: SA16195, July 25, 2005<br>Slackware Security Advisory, SSA:2005-203-03, July 22, 2005<br>FreeBSD Security Advisory, SA-05:18, July 27, 2005<br>SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005<br>Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005<br>Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005<br>Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005<br>Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005<br>Turbolinux Security Advisory, TLSA-2005-83, August 18, 2005<br>SCO Security Advisory, SCOSA-2005.33, August 19, 2005<br>Debian Security Advisory, DSA 797-1, September 1, 2005<br>Security Focus, Bugtraq ID: 14340, September 12, 2005<br>Fedora Legacy Update Advisory, |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | FLSA:162680, September 14, 2005<br>Debian Security Advisory, DSA 797-2, September 29, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:196, October 26, 2005<br>Ubuntu Security Notice, USN-151-3, October 28, 2005<br>Ubuntu Security Notice, USN-151-4, November 09, 2005<br>**SCO Security Advisory, SCOSA-2006.6, January 10, 2006** |
| Multiple Vendors<br>KDE kword 1.4.2, kpdf 3.4.3, 3.2, KOffice 1.4-1.4.2, kdegraphics 3.4.3, 3.2;<br>Gentoo Linux | Multiple buffer and integer overflows have been reported, which could let a remote malicious user execute arbitrary code.<br>Gentoo<br>Ubuntu<br>Fedora<br>Mandriva<br>Ubuntu<br>Debian<br>Debian<br>Currently we are not aware of any exploits for this vulnerability. | KPdf & KWord Multiple Unspecified Buffer & Integer Overflow<br>CVE-2005-3624<br>CVE-2005-3625<br>CVE-2005-3626<br>CVE-2005-3627 | Not available | Gentoo Linux Security Advisory GLSA 200601-02, January 5, 2006<br>Ubuntu Security Notice, USN-236-1, January 05, 2006<br>Fedora Update Notifications, FEDORA-2005-000, January 5, 2006<br>Mandriva Linux Security Advisories MDKSA-2006:003-003-006 & 008, January 6 & 7, 2006<br>Ubuntu Security Notice, USN-236-2, January 09, 2006<br>Debian Security Advisory DSA 931-1, January 9, 2006<br>Debian Security Advisory, DSA-936-1, January 11, 2006 |
| Multiple Vendors<br>Larry Wall Perl 5.8, 5.8.1, 5.8.3, 5.8.4, 5.8.4 -1-5.8.4-5; Ubuntu Linux 4.1 ppc, ia64, ia32 | Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PERLIO_DEBUG' SuidPerl environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists due to an error when handling debug message output, which could let a malicious user corrupt arbitrary files.<br>Ubuntu<br>Gentoo<br>Mandrake<br>RedHat<br>SGI<br>SUSE<br>Trustix<br>IBM<br>Fedora<br>**Conectiva**<br>Proofs of Concept exploits have been published. | Perl SuidPerl Multiple Vulnerabilities<br>CVE-2005-0155<br>CVE-2005-0156 | 4.9<br>(CVE-2005-0155)<br>2.3<br>(CVE-2005-0156) | Ubuntu Security Notice, USN-72-1, February 2, 2005<br>MandrakeSoft Security Advisory, MDKSA-2005:031, February 9, 2005<br>RedHat Security Advisory, RHSA-2005:105-11, February 7, 2005<br>SGI Security Advisory, 20050202-01-U, February 9, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005<br>Gentoo Linux Security Advisory, GLSA 200502-13, February 11, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0003,February 11, 2005<br>IBM SECURITY ADVISORY, February 28, 2005<br>Fedora Update Notification, FEDORA-2005-353, May 2, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1056, January 2, 2006** |
| Multiple Vendors<br>Linux kernel | A vulnerability has been reported in the 'restore_sigcontext()' function due to a failure to restrict access to the 'ar.rsc' register, which could let | Linux Kernel 64 Bit 'AR-RSC' Register | 2.3 | Security Tracker Alert ID: 1014275, June 23, 2005 |

| | | | | |
|---|---|---|---|---|
| 2.6 prior to 2.6.12.1 | a malicious user cause a Denial of Service or obtain elevated privileges.<br>Linux Kernel<br>SUSE<br>RedHat:<br>RedHat<br>Debian<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Access<br>CVE-2005-1761 | | SUSE Security Announcement, SUSE-SA:2005:044, August 4, 2005<br>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Debian Security Advisories, DSA 921-1 & 922-1, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6.8, 2.6.10 | A remote Denial of Service vulnerability has been reported in the 'ipt_recent' module when specially crafted packets are sent.<br>Ubuntu<br>Mandriva<br>RedHat<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel 'Ipt_recent' Remote Denial of Service<br>CVE-2005-2872 | 3.3 | Security Focus, Bugtraq ID: 14791, September 9, 2005<br>Ubuntu Security Notice, USN-178-1, September 09, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6.8-2.6.10, 2.4.21 | Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in 'msg_control' when copying 32 bit contents, which could let a malicious user obtain root privileges and execute arbitrary code; and a vulnerability was reported in the 'raw_sendmsg()' function, which could let a malicious user obtain sensitive information or cause a Denial of Service.<br>Ubuntu<br>Trustix<br>Fedora<br>RedHat<br>Mandriva<br>RedHat<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for these vulnerabilities. | Linux Kernel Buffer Overflow, Information Disclosure, & Denial of Service<br>CVE-2005-2490<br>CVE-2005-2492 | 4.9<br>(CVE-2005-2490)<br>4.7<br>(CVE-2005-2492) | Secunia Advisory: SA16747, September 9, 2005<br>Ubuntu Security Notice, USN-178-1, September 09, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0049, September 16, 2005<br>Fedora Update Notifications, FEDORA-2005-905 & 906, September 22, 2005<br>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |

|  |  |  |  |  |
|---|---|---|---|---|
| Multiple Vendors<br>Linux kernel 2.6-2.6.12 .1 | A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies.<br>Ubuntu<br>This issue has been addressed in Linux kernel 2.6.13-rc7.<br>SUSE<br>RedHat<br>RedHat<br>Mandriva<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel IPSec Policies Authorization Bypass<br>CVE-2005-2555 | 4.9 | Ubuntu Security Notice, USN-169-1, August 19, 2005<br>Security Focus, Bugtraq ID 14609, August 19, 2005<br>Security Focus, Bugtraq ID 14609, August 25, 2005<br>SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005<br>RedHat Security Advisory, RHSA-2005:663-19, September 28, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6-2.6.12 .3, 2.4-2.4.32 | A Denial of Service vulnerability has been reported in 'IP_VS_CONN_FLUSH' due to a NULL pointer dereference.<br>Kernel versions 2.6.13 and 2.4.32-pre2 are not affected by this issue.<br>Ubuntu<br>Mandriva<br>Debian<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel Denial of Service<br>CVE-2005-3274 | 2.3 | Security Focus, Bugtraq ID: 15528, November 22, 2005<br>Ubuntu Security Notice, USN-219-1, November 22, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>Debian Security Advisory, DSA 922-1, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6-2.6.12, 2.4-2.4.31 | A remote Denial of Service vulnerability has been reported due to a design error in the kernel.<br>The vendor has released versions 2.6.13 and 2.4.32-rc1 of the kernel to address this issue.<br>Ubuntu<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel Remote Denial of Service<br>CVE-2005-3275 | 3.3 | Ubuntu Security Notice, USN-219-1, November 22, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6-2.6.13.1 | A Denial of Service vulnerability has been reported due to an omitted call to the 'sockfd_put()' function in the 32-bit compatible 'routing_ioctl()' function.<br>Linux Kernel<br>Ubuntu<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel routing_ioctl() Denial of Service<br>CVE-2005-3044 | 2.3 | Security Tracker Alert ID: 1014944, September 21, 2005<br>Ubuntu Security Notice, USN-187-1, September 25, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219, 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |

| | | | | |
|---|---|---|---|---|
| Multiple Vendors<br>Linux kernel 2.6-2.6.14 | Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to a memory leak in '/security/keys/request_ key_auth.c;' a Denial of Service vulnerability was reported due to a memory leak in '/fs/namei.c' when the 'CONFIG_AUDITSYSCALL' option is enabled; and a vulnerability was reported because the orinoco wireless driver fails to pad data packets with zeroes when increasing the length, which could let a malicious user obtain sensitive information.<br>Linux Kernel<br>Fedora<br>Trustix<br>RedHat<br>Ubuntu<br>Mandriva<br>SUSE<br>**Conectiva**<br>There is no exploit code required. | Linux Kernel Denial of Service & Information Disclosure<br>CVE-2005-3119<br>CVE-2005-3180<br>CVE-2005-3181 | 2.3 (CVE-2005-3119)<br>3.3 (CVE-2005-3180)<br>2.3 (CVE-2005-3181) | Secunia Advisory: SA17114, October 12, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005<br>Fedora Update Notifications, FEDORA-2005-1013, October 20, 2005<br>RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005<br>Ubuntu Security Notice, USN-219-1, November 22, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6-2.6.14 | Several vulnerabilities have been reported: a Denial of Service vulnerability was reported when handling asynchronous USB access via usbdevio; and a Denial of Service vulnerability was reported in the 'ipt_recent.c' netfilter module due to an error in jiffies comparison.<br>RedHat<br>Ubuntu<br>Mandriva<br>SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for these vulnerabilities. | Linux Kernel USB Subsystem Denials of Service<br>CVE-2005-2873<br>CVE-2005-3055 | 2.3 (CVE-2005-2873)<br>2.3 (CVE-2005-3055) | Secunia Advisory: SA16969, September 27, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Ubuntu Security Notice, USN-219-1, November 22, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:067, December 6, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux Kernel 2.6-2.6.14 | Multiple vulnerabilities have been reported: a Denial of Service vulnerability was reported in the 'sys_set_ mempolicy' function when a malicious user submits a negative first argument; a Denial of Service vulnerability was reported when threads are sharing memory mapping via 'CLONE_VM'; a Denial of Service vulnerability was reported in 'fs/exec.c' when one thread is tracing another thread that shares the same memory map; a Denial of Service vulnerability was reported in 'mm/ioremap.c' when performing a lookup of a non-existent page; a Denial of Service vulnerability was reported in the HFS and HFS+ (hfsplus) modules; and a remote Denial of Service vulnerability was reported due to a race condition in 'ebtables.c' when running on a SMP system that is operating under a heavy load.<br>Ubuntu<br>Trustix<br>RedHat<br>Mandriva | Multiple Vendors Linux Kernel Denials of Service<br>CVE-2005-3053<br>CVE-2005-3106<br>CVE-2005-3107<br>CVE-2005-3108<br>CVE-2005-3109<br>CVE-2005-3110 | 2.3 (CVE-2005-3053)<br>2.3 (CVE-2005-3106)<br>2.3 (CVE-2005-3107)<br>2.3 (CVE-2005-3108)<br>2.3 (CVE-2005-3109)<br>3.3 (CVE-2005-3110) | Ubuntu Security Notice, USN-199-1, October 10, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0057, October 14, 2005<br>RedHat Security Advisory, RHSA-2005:808-14, October 27, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005: 219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |

| | | | | |
|---|---|---|---|---|
| | SUSE<br>**Conectiva**<br>Currently we are not aware of any exploits for these vulnerabilities. | | | |
| Multiple Vendors<br>Linux kernel 2.6-2.6.14, 2.5.0-2.5.69, 2.4-2.4.32, 2.3, 2.3.x, 2.3.99, pre1-pre7, 2.2-2.2.27, 2.1, 2.1 .x, 2.1.89, 2.0.28-2.0.39 | A vulnerability has been reported due to the way console keyboard mapping is handled, which could let a malicious user modify the console keymap to include scripted macro commands.<br>Mandriva<br>Fedora<br>**Conectiva**<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | Linux Kernel Console Keymap Arbitrary Command Injection<br>CVE-2005-3257 | 4.9 | Security Focus, Bugtraq ID: 15122, October 17, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005<br>Fedora Update Notification, FEDORA-2005-1138, December 13, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Linux kernel 2.6-2.6.12 .1 | Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling key rings; and a Denial of Service vulnerability was reported in the 'KE YCTL_JOIN_SESSION _KEYRING' operation due to an error when attempting to join a key management session.<br>Linux Kernel<br>Ubuntu<br>Trustix<br>RedHat<br>Mandriva<br>**Conectiva**<br>There is no exploit code required. | Linux Kernel Management Denials of Service<br>CVE-2005-2098<br>CVE-2005-2099 | 3.3 (CVE-2005-2098)<br>3.3 (CVE-2005-2099) | Secunia Advisory: SA16355, August 9, 2005<br>Ubuntu Security Notice, USN-169-1, August 19, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005<br>RedHat Security Advisory, RHSA-2005:514-46, October 5, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:220, November 30, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Network Block Device NBD 2.8-2.8.2, 2.7.5;<br>Gentoo Linux;<br>Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha | A buffer overflow vulnerability has been reported in the 'nbd-server' when handling specially crafted requests, which could let a remote malicious user execute arbitrary code.<br>Upgrades available<br>Debian<br>Gentoo<br>**Ubuntu**<br>Currently we are not aware of any exploits for this vulnerability. | Multiple Vendors Network Block Device Server Buffer Overflow<br>CVE-2005-3534 | 7 | Security Focus, Bugtraq ID: 16029, December 21, 2005<br>Debian Security Advisory, DSA 924-1, December 21, 2005<br>Gentoo Linux Security Advisory, GLSA 200512-14, December 23, 2006<br>**Ubuntu Security Notice, USN-237-1, January 06, 2006** |
| Multiple Vendors<br>petris 1.0.1 | A buffer overflow vulnerability has been reported when handling environment variables when processing highscores, which could let a malicious user execute arbitrary code.<br>Debian<br>Currently we are not aware of any exploits for this vulnerability. | Petris Buffer Overflow<br>CVE-2005-3540 | 8 | Debian Security Advisory, DSA-929-1, January 9, 2006 |
| Multiple Vendors<br>RedHat Enterprise Linux WS 4, WS 3, ES 4, ES 3, AS 4, AS 3, Desktop 4.0, 3.0; mod_auth_pgsql 2.0.1 | A format string vulnerability has been reported in 'mod_auth_pgsql' when logging information, which could let a remote malicious user execute arbitrary code.<br>mod_auth_pgsql<br>RedHat<br>Fedora<br>Mandriva<br>Ubuntu<br>Currently we are not aware of any exploits for this | Multiple Vendors mod_auth_pgsql Apache Module Format String<br>CVE-2005-3656 | Not available | RedHat Security Advisory, RHSA-2006:0164-7, January 5, 2006<br>Fedora Update Notifications, FEDORA-2005-014 & 015, January 6, 2005<br>Mandriva Linux Security Advisory, MDKSA-2006:009, January 7, 2006<br>Ubuntu Security Notice, USN-239-1, January 09, 2006 |

|  |  |  |  |  |
|---|---|---|---|---|
|  | vulnerability. |  |  |  |
| Multiple Vendors<br>RedHat Fedora Core3; Linux kernel 2.6.10-2.6.13 | A vulnerability has been reported because a world writable file is created in 'SYSFS' which could let a malicious user obtain sensitive information.<br>Linux Kernel<br>Fedora<br>Mandriva<br>**Conectiva**<br>There is no exploit code required. | Linux Kernel World Writable SYSFS Information Disclosure<br>CVE-2005-3179 | 2.3 | Security Focus, Bugtraq ID: 15154, October 20, 2005<br>Fedora Update Notification FEDORA-2005-1007, October 20, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:220, November 30, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Stefan Frings SMS Server Tools 1.14.8;<br>Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha, | A format string vulnerability has been reported in 'logging.c' when attempting to log messages using a formatted print function, which could let a remote malicious user execute arbitrary code.<br>Debian<br>Currently we are not aware of any exploits for this vulnerability. | Stefan Frings SMS Server Tools Format String<br>CVE-2006-0083 | 5.6 | Security Focus, Bugtraq ID: 16188, January 9, 2006<br>Debian Security Advisory, DSA-930-2, January 9, 2006 |
| Multiple Vendors<br>Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;<br>Linux kernel 2.6.10, rc2, 2.6.8, rc1 | A remote Denial of Service vulnerability has been reported in the kernel driver for compressed ISO file systems when attempting to mount a malicious compressed ISO image.<br>Ubuntu<br>SUSE<br>Mandriva<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel ISO File System Remote Denial of Service<br>CVE-2005-2457 | 3.3 | Ubuntu Security Notice, USN-169-1, August 19, 2005<br>SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:218, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;<br>Trustix Secure Linux 3.0, 2.2, Trustix Secure Enterprise Linux 2.0;<br>SuSE Novell Linux Desktop 9.0, Linux Professional 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Personal 9.3 x86_64, 9.3, 9.2 x86_64, 9.2, 9.1 x86_64, 9.1, Linux Enterprise Server 9;<br>Linux kernel 2.6-2.6.12 .4 | A Denial of Service vulnerability has been reported due to a failure to handle exceptional conditions.<br>Linux Kernel<br>Ubuntu<br>SUSE<br>Trustix<br>Mandriva<br>Mandriva:<br>SUSE:<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel ZLib Invalid Memory Access Denial of Service<br>CVE-2005-2458 | 3.3 | SUSE Security Announcement, SUSE-SA:2005:050, September 1, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0043, September 2, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:171, October 3, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:219 & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.0 4, i386, amd64, 4.1 ppc, ia64, ia32;<br>Linux kernel 2.6-2.6.13 | A Denial of Service vulnerability has been reported in the '/proc/scsi/sg/devices' file due to a memory leak.<br>Ubuntu<br>Mandriva<br>SUSE<br>**Conectiva**<br>A Proof of Concept exploit has been published. | Linux Kernel SCSI ProcFS Denial of Service<br>CVE-2005-2800 | 2.3 | Security Focus, Bugtraq ID: 14790, September 9, 2005<br>Ubuntu Security Notice, USN-178-1, September 09, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219, & 220, November 30, 2005<br>SUSE Security Announcement, SUSE-SA:2005:068, December 14, 2005<br>**Conectiva Linux** |

| | | | | |
|---|---|---|---|---|
| | | | | **Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.10 powerpc, i386, amd64, 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32;<br>IBM HTTP Server 2.0.47.1, 2.0.47, 2.0.42.2, 2.0.42.1, 2.0.42;<br>Apache 2.0.28-2.0.54, 2.0 a9, 2.0 | A remote Denial of Service vulnerability has been reported in 'worker.c' due to a memory leak.<br>Apache<br>Ubuntu<br>IBM<br>**RedHat**<br>There is no exploit code required. | Apache MPM 'Worker.C' Remote Denial of Service<br>CVE-2005-2970 | 3.3 | Security Focus, Bugtraq ID: 15762, December 7, 2005<br>Ubuntu Security Notice, USN-225-1, December 06, 2005<br>**RedHat Security Advisory, RHSA-2006:0159-8, January 5, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.10 powerpc, i386, amd64;<br>Linux kernel 2.6-2.6.12 .3 | An information disclosure vulnerability has been reported in 'SYS_GET_THREAD _AREA,' which could let a malicious user obtain sensitive information.<br>Kernel versions 2.6.12.4 and 2.6.13 are not affected by this issue.<br>Ubuntu<br>Mandriva<br>Debian<br>**Conectiva**<br>Currently we are not aware of any exploits for this vulnerability. | Linux Kernel Information Disclosure<br>CVE-2005-3276 | 2.3 | Ubuntu Security Notice, USN-219-1, November 22, 2005<br>Mandriva Linux Security Advisories, MDKSA-2005:218, 219 & 220, November 30, 2005<br>Debian Security Advisory, DSA 922-1, December 14, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1059, January 2, 2006** |
| Multiple Vendors<br>Webmin 0.88 -1.230, 0.85, 0.76-0.80, 0.51, 0.42, 0.41, 0.31, 0.22, 0.21, 0.8.5 Red Hat, 0.8.4, 0.8.3, 0.1-0.7; Usermin 1.160, 1.150, 1.140, 1.130, 1.120, 1.110, 1.0, 0.9-0.99, 0.4-0.8; Larry Wall Perl 5.8.3-5.8.7, 5.8.1, 5.8 .0-88.3, 5.8, 5.6.1, 5.6, 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03 | A format string vulnerability has been reported in 'Perl_sv_ vcatpvfnl' due to a failure to properly handle format specifiers in formatted printing functions, which could let a remote malicious user cause a Denial of Service.<br>Webmin<br>Fedora<br>OpenPKG<br>Mandriva<br>Ubuntu<br>Gentoo<br>Gentoo<br>Mandriva<br>SUSE<br>Trustix<br>Ubuntu<br>Fedora<br>RedHat<br>**OpenBSD**<br>OpenBSD<br>An exploit has been published. | Perl 'miniserv.pl' script Format String<br>CVE-2005-3912<br>CVE-2005-3962 | 9.3<br>(CVE-2005-3212)<br>6<br>(CVE-2005-3962) | Security Focus, Bugtraq ID: 15629, November 29, 2005<br>Fedora Update Notifications, FEDORA-2005-1113, 1116, & 1117, December 1 & 2, 2005<br>OpenPKG Security Advisory, OpenPKG-SA-2005.025, December 3, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:223, December 2, 2005<br>Ubuntu Security Notice, USN-222-1 December 02, 2005, December 2, 2005<br>Gentoo Linux Security Advisory, GLSA 200512-01 & 200512-02, December 7, 2005<br>US-CERT VU#948385<br>Mandriva Linux Security Advisory, MDKSA-2005:225, December 8, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:029, December 9, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0070, December 9, 2005<br>Ubuntu Security Notice, USN-222-2, December 12, 2005<br>Fedora Update Notifications, FEDORA-2005-1144 & 1145, December 14, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:030, December 16, 2005<br>RedHat Security Advisory, RHSA-2005:880-8, December 20, 2005<br>**Security Focus, Bugtraq ID:** |

| | | | | |
|---|---|---|---|---|
| | | | | **15629, January 4, 2006** |
| Multiple Vendors<br>X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0 | An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code.<br>Patch available<br>Gentoo<br>Ubuntu<br>Gentoo<br>Ubuntu<br>ALTLinux<br>Fedora<br>RedHat<br>SGI<br>RedHat<br>Mandrake<br>Mandriva<br>Debian<br>RedHat<br>RedHat<br>RedHat<br>Apple<br>Fedora<br>SCO<br>**SCO**<br>**FedoraLegacy**<br>Currently we are not aware of any exploits for this vulnerability. | LibXPM Bitmap_unit Integer Overflow<br>CVE-2005-0605 | 7 | Security Focus, 12714, March 2, 2005<br>Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005<br>Ubuntu Security Notice, USN-92-1 March 07, 2005<br>Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005<br>Ubuntu Security Notice, USN-97-1 March 16, 2005<br>ALTLinux Security Advisory, March 29, 2005<br>Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005<br>RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005<br>SGI Security Advisory, 20050401-01-U, April 6, 2005<br>RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005<br>Debian Security Advisory, DSA 723-1, May 9, 2005<br>RedHat Security Advisory, RHSA-2005:412-05, May 11, 2005<br>RedHat Security Advisory, RHSA-2005:473-03, May 24, 2005<br>RedHat Security Advisory, RHSA-2005:198-35, June 8, 2005<br>Fedora Update Notifications, FEDORA-2005-808 & 815, August 25 & 26, 2005<br>SCO Security Advisory, SCOSA-2005.57, December 14, 2005<br>**SCO Security Advisory, SCOSA-2006.5, January 4, 2006**<br>**Fedora Legacy Update Advisory, FLSA:152803, January 10, 2006** |
| NetBSD<br>NetBSD 2.1, 2.0-2.0.3, 1.6- 1.6.2, NetBSD Current | A vulnerability has been reported in the 'kernfs' file system due to insufficient sanitization, which could let a malicious user obtain sensitive information.<br>NetBSD | NetBSD KernFS Memory Disclosure<br>CVE-2006-0145 | 4.9 | NetBSD Security Advisory, 2006-001, January 9, 2006 |

| | | | | |
|---|---|---|---|---|
| | Currently we are not aware of any exploits for this vulnerability. | | | |
| netpbm<br>10.0 | A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code.<br>Trustix<br>Gentoo<br>Mandriva<br>Ubuntu<br>Fedora<br>SUSE<br>RedHat<br>SGI<br>Conectiva<br>TurboLinux<br>**Fedora**<br>There is no exploit code required. | netpbm Arbitrary Code Execution<br>CVE-2005-2471 | 7 | Secunia Advisory: SA16184, July 25, 2005<br>Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005<br>Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:133, August 10, 2005<br>Ubuntu Security Notice, USN-164-1, August 11, 2005<br>Fedora Update Notifications, FEDORA-2005-727 & 728, August 17, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005<br>RedHat Security Advisory, RHSA-2005:743-08, August 22, 2005<br>SGI Security Advisory, 20050901-01-U, September 7, 2005<br>**Conectiva Linux Announcement, CLSA-2005:1007, September 13, 2005**<br>Turbolinux Security Advisory, TLSA-2005-90, September 20, 2005<br>**Fedora Update Notification, FEDORA-2005-000, January 5, 2006** |
| OpenBSD<br>OpenBSD 3.8, 3.7 | A vulnerability has been reported in '/dev/fd' due to an unspecified error, which could let a malicious user obtain unauthorized access.<br>OpenBSD<br>Currently we are not aware of any exploits for this vulnerability. | OpenBSD DEV/FD Unauthorized File Access<br>CVE-2006-0098 | 4.9 | Security Focus, Bugtraq ID: 16144, January 5, 2006 |
| PHP go-pear.php<br>PHP go-pear.php0.2.2 | A vulnerability has been reported that could let a remote malicious user execute arbitrary code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | PHP PEAR Go-Pear.PHP Arbitrary Remote Code Execution<br>CVE-2006-0144 | 8 | Security Focus, Bugtraq ID: 16174, January 9, 2006 |
| PostgreSQL<br>PostgreSQL 8.1, 8.0-8.0.2, 7.4.3-7.4.9, 7.4, 7.3 -7.3.9 | A remote Denial of Service vulnerability has been reported due to a failure to properly handle exceptional conditions.<br>Postgresql<br>There is no exploit code required. | PostgreSQL Postmaster Denial of Service<br>CVE-2006-0105 | 2.3 | Security Focus, Bugtraq ID: 16201, January 11, 2006 |
| Qualcomm<br>Eudora Internet Mail Server for OS X Light 3.2.8, 3.2.4-3.2.6, Mail Server for OS X3.2.4-3.2.8 | Denial of service vulnerabilities have been reported when a malformed NTLM authentication request, corrupted incoming Mail X, or malformed temporary mail is submitted.<br>Patches available<br>Currently we are not aware of any exploits for this vulnerability. | Qualcomm Eudora Internet Mail Server Denial of Service<br>CVE-2006-0141 | Not available | Secunia Advisory: SA18356, January 9, 2006 |

| | | | | |
|---|---|---|---|---|
| Sun Microsystems, Inc.<br>Solaris 9.0 _x86, 9.0, 8.0 _x86, 8.0 | A buffer overflow vulnerability has been reported due to an unspecified error in the uucp(1C) and uustat(1C) utilities, which could let a malicious user execute arbitrary code.<br>Sun<br>Currently we are not aware of any exploits for this vulnerability. | Sun Solaris UUSTAT Buffer Overflow<br>CVE-2004-0780<br>CVE-2006-0161 | 5.6<br>(CVE-2006-0161) | Sun(sm) Alert Notification, Sun Alert ID: 101933, January 9, 2006 |
| Todd Miller<br>Sudo 1.x | A vulnerability has been reported in the environment cleaning due to insufficient sanitization, which could let a malicious user obtain elevated privileges.<br>Debian<br>Mandriva<br>Ubuntu<br>SUSE<br>Trustix<br>**Conectiva**<br>An exploit script has been published. | Todd Miller Sudo Local Elevated Privileges<br>CVE-2005-2959 | 4.9 | Debian Security Advisory, DSA 870-1, October 25, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:201, October 27, 2005<br>Ubuntu Security Notice, USN-213-1, October 28, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005<br>Security Focus, Bugtraq ID: 15191, November 10, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0062, November 22, 2005<br>**Conectiva Linux Announcement, CLSA-2006:1057, January 2, 2006** |
| Todd Miller<br>Sudo prior to 1.6.8p12 | A vulnerability has been reported due to an error when handling the 'PERLLIB,' 'PERL5LIB,' and 'PERL5OPT' environment variables when tainting is ignored, which could let a malicious user bypass security restrictions and include arbitrary library files.<br>Updates available at:<br>Sudo<br>Mandriva<br>**Ubuntu**<br>There is no exploit code required; however, a Proof of Concept exploit script has been published. | Todd Miller Sudo Security Bypass<br>CVE-2005-4158 | 4.9 | Security Focus, Bugtraq ID: 15394, November 11, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:234, December 20, 2005<br>**Ubuntu Security Notice, USN-235-1, January 05, 2006** |
| University of Washington<br>UW-imapd imap-2004c1 | A buffer overflow has been reported in UW-imapd that could let remote malicious users cause a Denial of Service or execute arbitrary code.<br>Upgrade to version imap-2004g<br>Trustix<br>Debian<br>Gentoo<br>SUSE<br>Mandriva<br>Slackware<br>Conectiva<br>RedHat<br>RedHat<br>Fedora<br>**Trustix**<br>Currently we are not aware of any exploits for this vulnerability. | UW-imapd Denial of Service and Arbitrary Code Execution<br>CVE-2005-2933 | 7 | Secunia, Advisory: SA17062, October 5, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0055, October 7, 2005<br>Debian Security Advisory, DSA 861-1, October 11, 2005<br>Gentoo Linux Security Advisory, GLSA 200510-10, October 11, 2005<br>US-CERT VU#933601<br>SUSE Security Summary Report, SUSE-SR:2005:023, October 14, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:189 & 194, October 21 & 26, 2005<br>Slackware Security Advisory, SSA:2005-310-06, November 7, 2005<br>Conectiva Linux Announcement, CLSA-2005:1046, November 21, 2005<br>RedHat Security Advisory, RHSA-2005:848-6 & 850-5, December 6, 2005 |

| | | | | |
|---|---|---|---|---|
| | | | | Fedora Update Notifications, FEDORA-2005-1112 & 1115, December 8, 2005<br>**Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005** |
| WebFTP for SysCP<br>WebFTP for SysCP 1.2.6 | A file include vulnerability has been reported, which could let a remote malicious user view unauthorized files and execute arbitrary scripts.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | SysCP WebFTP Module File Include<br>CVE-2006-0132 | 7 | Security Focus, Bugtraq ID: 16175, January 9, 2006 |
| Xmame<br>Xmame 0.102 | Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in the 'lang' command line option due to a boundary error, which could let a malicious user execute arbitrary code; and a buffer overflow vulnerability was reported when handling the 'lang,' 'ctrlr,' 'pb,' and 'rec' command line options, which could let a malicious user execute arbitrary code.<br>The vulnerabilities have been fixed in the CVS repositories.<br>Proof of Concept exploits, xmameOverflow-ruby.txt, have been published. | Xmame Buffer Overflows<br>CVE-2006-0176 | Not available | Secunia Advisory: SA8931, January 11, 2006 |

[back to top]

## Multiple Operating Systems - Windows / UNIX / Linux / Other

| Vendor & Software Name | Vulnerability - Impact<br>Patches - Workarounds<br>Attack Scripts | Common Name / CVE Reference | Risk | Source |
|---|---|---|---|---|
| 427BB<br>fourtwosevenbb 2.2.1, 2.2 | An SQL injection vulnerability has been reported in 'showthread.php' due to insufficient sanitization before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit, EV0018.txt, has been published. | 427BB SQL Injection<br>CVE-2006-0154 | 7 | Security Focus, Bugtraq ID: 16169, January 9, 2006 |
| 427BB<br>fourtwosevenbb 2.2.1, 2.2 | A vulnerability has been reported due to insufficient validation of user-supplied data, which could let a remote malicious user bypass authentication.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | 427BB Authentication Bypass<br>CVE-2006-0153 | 7 | Security Focus, Bugtraq ID: 16178, January 9, 2006 |
| ADN Forum<br>ADN Forum 1.0 b, 1.0 | Several input validation vulnerabilities have been reported: an SQL injection vulnerability was reported in 'index.php' due to insufficient sanitization of the 'fid' parameter and in 'verpag.php' due to insufficient sanitization of the 'pagid' parameter, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the 'titulo' parameter, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0015.txt, have been published. | ADN Forum SQL Injection & Cross-Site Scripting<br>CVE-2006-0123<br>CVE-2006-0124 | 7<br>(CVE-2006-0123)<br>2.3<br>(CVE-2006-0124) | Security Tracker Alert ID: 1015445, January 6, 2006 |
| Andromeda<br>Andromeda 1.9.3 .4 | A Cross-Site Scripting vulnerability has been reported in 'andromeda.php' due to insufficient sanitization of the 's' parameter before returning the user, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | Andromeda Cross-Site Scripting<br>CVE-2006-0142 | 2.3 | Secunia Advisory: SA18359, January 9, 2006 |

| | | | | |
|---|---|---|---|---|
| Apache Software Foundation<br>Apache prior to 1.3.35-dev, 2.0.56-dev | A Cross-Site Scripting vulnerability has been reported in the 'Referer' directive in 'mod_imap' due to insufficient sanitization before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.<br>The vulnerability has been fixed in version 1.3.35-dev, and 2.0.56-dev.<br>OpenPKG<br>Trustix<br>**Mandriva**<br>There is no exploit code required. | Apache mod_imap Cross-Site Scripting<br>CVE-2005-3352 | 2.3 | Security Tracker Alert ID: 1015344, December 13, 2005<br>OpenPKG Security Advisory, OpenPKG-SA-2005.029, December 14, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0074, December 23, 2005<br>**Mandriva Linux Security Advisory, MDKSA-2006:007, January 6, 2006** |
| Apple<br>AirPort Extreme Firmware 5.5, AirPort Express Firmware 6.1 | A remote Denial of Service vulnerability has been reported in the base station when handling certain network packets.<br>Update available<br>There is no exploit code required. | Apple AirPort Remote Denial of Service<br>CVE-2005-3714 | Not available | Apple Security Advisory, APPLE-SA-2006-01-05, January 5, 2006 |
| Apple<br>QuickTime Player 7.0-7.0.3 | Several vulnerabilities have been reported: a heap-based buffer overflow vulnerability was reported when handling 'QTIF' images due to a boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability was reported when handling 'TGA' images, which could let a remote malicious user execute arbitrary code; an integer overflow vulnerability was reported when handling 'TIFF' images, which could let a remote malicious user execute arbitrary code; a heap-based buffer overflow vulnerability was reported when handling 'GIF' images, which could let a remote malicious user execute arbitrary code; and a heap-based buffer overflow vulnerability was reported when handling certain media files, which could let a remote malicious user execute arbitrary code.<br>QuickTime<br>Currently we are not aware of any exploits for these vulnerabilities. | QuickTime Multiple Image/Media File Handling Vulnerabilities<br>CVE-2005-2340<br>CVE-2005-3707<br>CVE-2005-3708<br>CVE-2005-3709<br>CVE-2005-3710<br>CVE-2005-3711<br>CVE-2005-3713<br>CVE-2005-4092 | 8 (CVE-2005-2340)<br>8 (CVE-2005-3707)<br>8 (CVE-2005-3708)<br>9 (CVE-2005-3709)<br>8 (CVE-2005-3710)<br>8 (CVE-2005-3711)<br>8 (CVE-2005-3713)<br>7 (CVE-2005-4092) | Apple Security Advisory, APPLE-SA-2006-01-10, January 10, 2006<br>US-CERT VU#629845<br>US-CERT VU#913449<br>US-CERT VU#115729<br>US-CERT VU#150753<br>US-CERT VU#921193 |
| AppServ Open Project<br>AppServ Open Project 2.4.5 | A vulnerability has been reported due to insufficient verification of the 'appserv_root' parameter in 'appserv/main.php' before used to include files, which could let a remote malicious user execute arbitrary PHP code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit, EV0018.txt, has been published. | AppServ File Inclusion<br>CVE-2006-0125 | 2.3 | Secunia Advisory: SA18163, January 5, 2006 |
| CaLogic<br>CaLogic 1.2.2 | An HTML injection vulnerability has been reported in the title field when a new event is added due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | CaLogic HTML Injection<br>CVE-2006-0180 | 2.3 | Secunia Advisory: SA18417, January 11, 2006 |
| Cisco Systems<br>Cisco CS-MARS 4.1.2, 4.1 | A vulnerability has been reported because a default static administrative password is set during installation, which could let a malicious user obtain unauthorized administrative access.<br>Cisco CS-MARS<br>There is no exploit code required. | Cisco CS-MARS Default Administrative Password<br>CVE-2006-0181 | 7 | Cisco Security Advisory, Document ID: 68605, January 11, 2006 |
| Cisco Systems<br>Cisco IP Phone 7940 | A remote Denial of Service vulnerability has been reported when a large amount of TCP SYN packets are submitted to port 80.<br>No workaround or patch available at time of publishing.<br>A Proof of Concept exploit script, CiscoPhoneDos.pl.txt, has been published. | Cisco IP Phone 7940 Remote Denial of Service<br>CVE-2006-0179 | Not available | Security Focus, Bugtraq ID: 16200, January 10, 2006 |

| | | | | |
|---|---|---|---|---|
| Cray<br>UNICOS 9.0.2 .2 | A buffer overflow vulnerability has been reported due to insufficient bounds checking of command line parameters, which could let a malicious user execute arbitrary code with superuser privileges.<br>No workaround or patch available at time of publishing.<br>A Proof of Concept exploit has been published. | Cray UNICOS Buffer Overflow<br>CVE-2006-0177 | Not available | Security Focus, Bugtraq ID: 16205, January 10, 2006 |
| Dave Carrigan<br>auth_ldap 1.6 .0, 1.4 .x, 1.3 .x, 1.2 .x | A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before using in the format-specifier of a formatted printing function, which could let a remote malicious user execute arbitrary code.<br>Upgrade available<br>RedHat<br>Currently we are not aware of any exploits for this vulnerability. | Dave Carrigan Auth_LDAP Remote Format String<br>CVE-2006-0150 | 8 | Security Focus, Bugtraq ID: 16177, January 9, 2006<br>RedHat Security Advisory, RHSA-2006:0179-7, January 10, 2006 |
| Edgewall Software<br>Trac 0.9.2 | An HTML injection vulnerability has been reported in the WikiProcessor Wiki Content due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.<br>Trac<br>There is no exploit code required. | Trac HTML Injection<br>CVE-2005-4644 | Not available | Security Focus, Bugtraq ID: 16198, January 10, 2006 |
| Ethereal<br>Ethereal V0.10.11 | Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a Denial of Service or execute arbitrary code.<br>Upgrade available<br>Fedora<br>Mandriva<br>RedHat<br>SUSE<br>Avaya<br>SGI<br>Conectiva<br>Debian<br>**FedoraLegacy**<br>Currently we are not aware of any exploits for these vulnerabilities. | Ethereal Denial of Service or Arbitrary Code Execution<br>CVE-2005-2361<br>CVE-2005-2362<br>CVE-2005-2363<br>CVE-2005-2364<br>CVE-2005-2365<br>CVE-2005-2366<br>CVE-2005-2367 | 3.3 (CVE-2005-2361)<br>3.3 (CVE-2005-2362)<br>3.3 (CVE-2005-2363)<br>3.3 (CVE-2005-2364)<br>3.3 (CVE-2005-2365)<br>3.3 (CVE-2005-2366)<br>8 (CVE-2005-2367) | Secunia, Advisory: SA16225, July 27, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005<br>RedHat Security Advisory, RHSA-2005:687-03, August 10, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005<br>Avaya Security Advisory, ASA-2005-185, August 30, 2005<br>SGI Security Advisory, 20050901-01-U, September 7, 2005<br>Conectiva Linux Announce-ment, CLSA-2005:1003, September 13, 2005<br>Debian Security Advisory, DSA 853-1, October 9, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |
| Ethereal Group<br>Ethereal 0.10-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7 | A buffer overflow vulnerability has been reported in the 'dissect_ospf_ v3_address_ prefix()' function in the OSPF protocol dissector due to a boundary error when converting received binary data to a human readable string, which could let a remote malicious user execute arbitrary code.<br>Patch available<br>Debian<br>Gentoo<br>Mandriva<br>**Fedora**<br>**RedHat**<br>Currently we are not aware of any exploits for this | Ethereal OSPF Protocol Dissection Buffer Overflow<br>CVE-2005-3651 | 8 | iDefense Security Advisory, December 9, 2005<br>Debian Security Advisory DSA 920-1, December 13, 2005<br>Gentoo Linux Security Advisory, GLSA 200512-06, December 14, 2005<br>Mandriva Linux Security Advisory MDKSA-2005:227, December 15, 2005<br>Mandriva Linux Security Advisory |

| | | | | |
|---|---|---|---|---|
| | vulnerability. | | | MDKSA-2006:002, January 3, 2006<br>**Fedora Update Notification FEDORA-2005-000, January 5, 2006**<br>**RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006** |
| Ethereal Group<br>Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9<br>Avaya Converged Communications Server (CCS) 2.x, Avaya S8XXX Media Servers | Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509.<br>Upgrades available<br>Gentoo<br>Mandriva<br>RedHat<br>Conectiva<br>SuSE<br>SGI<br>Avaya<br>**FedoraLegacy**<br>An exploit script has been published. | Ethereal Multiple Remote Protocol Dissector Vulnerabilities<br>CVE-2005-1456<br>CVE-2005-1457<br>CVE-2005-1458<br>CVE-2005-1459<br>CVE-2005-1460<br>CVE-2005-1461<br>CVE-2005-1462<br>CVE-2005-1463<br>CVE-2005-1464<br>CVE-2005-1465<br>CVE-2005-1466<br>CVE-2005-1467<br>CVE-2005-1468<br>CVE-2005-1469<br>CVE-2005-1470 | 3.3<br>(CVE-2005-1456)<br>3.3<br>(CVE-2005-1457)<br>2.3<br>(CVE-2005-1458)<br>3.3<br>(CVE-2005-1459)<br>3.3<br>(CVE-2005-1460)<br>8<br>(CVE-2005-1461)<br>7<br>(CVE-2005-1462)<br>7<br>(CVE-2005-1463)<br>3.3<br>(CVE-2005-1464)<br>3.3<br>(CVE-2005-1465)<br>3.3<br>(CVE-2005-1466)<br>3.3<br>(CVE-2005-1467)<br>3.3<br>(CVE-2005-1468)<br>3.3<br>(CVE-2005-1469)<br>3.3<br>(CVE-2005-1470) | Ethereal Security Advisory, enpa-sa-00019, May 4, 2005<br>Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:083, May 11, 2005<br>RedHat Security Advisory, RHSA-2005:427-05, May 24, 2005<br>Conectiva Security Advisory, CLSA-2005:963, June 6, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005<br>SGI Security Advisory, 20050503-01-U, June 8, 2005<br>Avaya Security Advisory, ASA-2005-131, June 13, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |
| Ethereal Group<br>Ethereal 0.9.1-0.10.13. | A remote Denial of Service vulnerability has been reported in the IRC and GTP dissectors when a malicious user submits a specially crafted packet.<br>Upgrades available<br>Mandriva<br>**RedHat**<br>Currently we are not aware of any exploits for this vulnerability. | Ethereal IRC & GTP Dissectors Remote Denial of Service<br>CVE-2005-4585 | 3.3 | Ethereal Security Advisory, enpa-sa-00022, December 27, 2005<br>Mandriva Linux Security Advisory MDKSA-2006:002, January 3, 2006<br>**RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006** |

| | | | | |
|---|---|---|---|---|
| Ethereal Group<br>Ethereal 0.10-0.10.8 | A buffer overflow vulnerability exists due to a failure to copy network derived data securely into sensitive process buffers, which could let a remote malicious user execute arbitrary code.<br>Upgrades available<br>Gentoo<br>Fedora<br>Mandrake<br>RedHat<br>ALT Linux<br>Conectiva<br>Avaya<br>**FedoraLegacy**<br>Exploit scripts have been published. | Ethereal Buffer Overflow<br>CVE-2005-0699 | 7 | Security Focus, 12759, March 8, 2005<br>Security Focus, 12759, March 14, 2005<br>Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005<br>Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005<br>Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005<br>RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005<br>Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005<br>ALTLinux Security Advisory, March 29, 2005<br>Avaya Security Advisory, ASA-2005-131, June 13, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |
| Ethereal Group<br>Ethereal 0.9-0.9.16, 0.10-0.10.9 | Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors.<br>Upgrades available<br>Gentoo<br>Fedora<br>Mandrake<br>RedHat<br>ALT Linux<br>Conectiva<br>Debian<br>Avaya<br>**FedoraLegacy**<br>A Denial of Service Proof of Concept exploit script has been published. | Ethereal Etheric/ GPRS-LLC/IAPP/ JXTA/s Flow Dissector Vulnerabilities<br>CVE-2005-0704<br>CVE-2005-0705<br>CVE-2005-0739<br>CVE-2005-0765<br>CVE-2005-0766 | 8<br>(CVE-2005-0704)<br>3.3<br>(CVE-2005-0705)<br>3.3<br>(CVE-2005-0739)<br>3.3<br>(CVE-2005-0765)<br>3.3<br>(CVE-2005-0766) | Ethereal Advisory, enpa-sa-00018, March 12, 2005<br>Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005<br>Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005<br>Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005<br>RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005<br>Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005<br>ALTLinux Security Advisory, March 29, 2005<br>Debian Security Advisory, DSA 718-1, April 28, 2005<br>Avaya Security Advisory, ASA-2005-131, June 13, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |

| | | | | |
|---|---|---|---|---|
| foxrum<br>foxrum 4.0.4 f | Multiple script injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before including in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0020.txt, have been published. | Foxrum Multiple BBCode Tag Script Injection<br>CVE-2006-0156 | 2.3 | Security Focus, Bugtraq ID: 16172, January 9, 2006 |
| Globalissa<br>phpChamber | A Cross-Site Scripting vulnerability has been reported in 'search_result.php' due to insufficient sanitization of the 'needle' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required | PHPChamber Cross-Site Scripting<br>CVE-2006-0152 | 2.3 | Secunia Advisory: SA18360, January 9, 2006 |
| IBM<br>Lotus Notes 6.5-6.5.4, Lotus Domino Enterprise Server 6.5.4, 6.5.2, Lotus Domino 6.5.0-6.5.4 | Multiple vulnerabilities have been reported including unspecified potential security issues in 'Agents;' an unspecified boundary error in CD to MIME Conversion, which could lead to a Denial of Service; a stack overflow vulnerability in in Domino for AIX when evaluating a long formula in 'Design,' which could lead to a Denial of Service; a vulnerability due to unspecified errors in the Directory Services that could lead to a Denial of Service when performing LDAP searches; a vulnerability due to an unspecified error in the IMAP server which could lead to a Denial of Service; a vulnerability due to an unspecified error when compact is executed from the client could lead to a Denial of Service; and several vulnerabilities due to unspecified errors when handling corrupted bitmap images or when performing the 'Delete Attachment' action.<br>Update information<br>Some of these vulnerabilities do not required an exploit. | IBM Lotus Domino Denial of Service& Unspecified Vulnerabilities<br>CVE-2006-0117<br>CVE-2006-0118<br>CVE-2006-0119<br>CVE-2006-0120<br>CVE-2006-0121 | 2.3<br>(CVE-2006-0117)<br>2.3<br>(CVE-2006-0118)<br>4.9<br>(CVE-2006-0119)<br>2.3<br>(CVE-2006-0120)<br>3.3<br>(CVE-2006-0121) | Secunia Advisory: SA18328, January 6, 2006 |
| Idea Development ID Oy<br>Timecan CMS | An SQL injection vulnerability has been reported due to insufficient sanitization of the 'viewID' parameter and potentially other parameters in various scripts, which could let a remote malicious user execute arbitrary SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | Timecan CMS SQL Injection<br>CVE-2006-0107 | 7 | Security Focus, Bugtraq ID: 16159, January 6, 2006 |
| iNETstore Corporation<br>iNETstore Online | A Cross-Site Scripting vulnerability has been reported in 'search.inetstore' due to insufficient sanitization of the 'searchterm' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | iNETstore Ebusiness Software Cross-Site Scripting<br>CVE-2006-0116 | 2.3 | Security Focus, Bugtraq ID: 16156, January 6, 2006 |
| Javier Suarez Sanz<br>Foro Domus 2.10 | A Cross-Site Scripting and SQL injection vulnerability has been reported in 'escribir.php' due to insufficient sanitization of the 'email' parameter, which could let a remote malicious user execute arbitrary HTML and script code or SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0016.txt, have been published. | Foro Domus Cross-Site Scripting & SQL Injection<br>CVE-2006-0110 | Not available | Secunia Advisory: SA18327, January 6, 2006 |
| Joomla<br>Joomla 1.0-1.0.5 | An information disclosure vulnerability has been reported due to a failure to properly secure sensitive and privileged information, which could let a remote malicious user obtain sensitive information.<br>Contact the vendor for a temporary fix.<br>There is no exploit code required. | Joomla Vcard Access Information Disclosure<br>CVE-2006-0114 | 2.3 | Security Focus, Bugtraq ID: 16185, January 9, 2006 |
| Modular Merchant<br>Modular Merchant Shopping Cart Software | A Cross-Site Scripting vulnerability has been reported in 'category.php' due to insufficient sanitization of the 'cat' parameter before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required. | Modular Merchant Shopping Cart Cross-Site Scripting<br>CVE-2006-0109 | 2.3 | Secunia Advisory: SA18320, January 6, 2005 |

| | | | | |
|---|---|---|---|---|
| Mozilla.org<br>Netscape 8.0.3.3, 7.2;<br>Mozilla Firefox 1.5 Beta1, 1.0.6; Mozilla Browser 1.7.11; Mozilla Thunderbird 1.0.6 | A buffer overflow vulnerability has been reported due to an error when handling IDN URLs that contain the 0xAD character in the domain name, which could let a remote malicious user execute arbitrary code.<br>Patches available<br>RedHat<br>RedHat<br>Fedora<br>Ubuntu<br>Gentoo<br>Slackware<br>Gentoo<br>Conectiva<br>Fedora<br>Debian<br>TurboLinux<br>HP<br>Mandriva<br>HPSBUX01231 Rev1:<br>Preliminary Mozilla 1.7.12 available.<br>Netscape<br>Debian<br>Debian<br>HPSBUX01231 Rrev.2: HP-UX Mozilla Remote Unauthorized Execution of Privileged Code or Denial of Service (DoS)) is available detailing information on the availability of version 1.7.12.01 of Mozilla for various HP platforms. Users should see the referenced advisory or contact HP for further information.<br>**FedoraLegacy**<br>A Proof of Concept exploit script has been published. | Mozilla/Netscape/ Firefox Browsers Domain Name Buffer Overflow<br>CVE-2005-2871 | 8 | Security Focus, Bugtraq ID: 14784, September 10, 2005<br>RedHat Security Advisories, 769-8 & RHSA-2005:768-6, September 9, 2005<br>Fedora Update Notifications, FEDORA-2005-871-184, September 10, 2005<br>Ubuntu Security Notice, USN-181-1, September 12, 2005<br>US-CERT VU#573857<br>Gentoo Linux Security Advisory GLSA 200509-11, September 18, 2005<br>Security Focus, Bugtraq ID: 14784, September 22, 2005<br>Slackware Security Advisory, SSA:2005-269-01, September 26, 2005<br>Gentoo Linux Security Advisory [UPDATE], GLSA 200509-11:02, September 29, 2005<br>Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005<br>Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005<br>Debian Security Advisory, DSA 837-1, October 2, 2005<br>Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005<br>HP Security Bulletin, HPSBUX01231, October 3, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005<br>HP Security Bulletin, HPSBUX01231 Rev 1, October 12, 2005<br>Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005<br>HP Security Bulletin, HPSBUX01231 Rev 2, November 9, 2005<br>**Fedora Legacy Update Advisory, FLSA:168375, January 9, 2006** |
| Multiple Vendors<br>Mozilla Firefox 1.0-1.0.6; Mozilla Browser 1.7-1.7.11; Netscape Browser | Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when processing malformed XBM images, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when unicode sequences contain 'zero-width non-joiner' characters, which could let a | Mozilla Browser / Firefox Multiple Vulnerabilities<br>CVE-2005-2701<br>CVE-2005-2702 | 7<br>(CVE-2005-2701)<br>8<br>(CVE-2005-2702) | Mozilla Foundation Security Advisory, 2005-58, September 22, 2005<br>RedHat Security |

| | | | | |
|---|---|---|---|---|
| 8.0.3.3 | remote malicious user cause a Denial of Service or execute arbitrary code; a vulnerability was reported due to a flaw when making XMLHttp requests, which could let a remote malicious user spoof XMLHttpRequest headers; a vulnerability was reported because a remote malicious user can create specially crafted HTML that spoofs XML objects to create an XBL binding to execute arbitrary JavaScript with elevated (chrome) permissions; an integer overflow vulnerability was reported in the JavaScript engine, which could let a remote malicious user obtain unauthorized access; a vulnerability was reported because a remote malicious user can load privileged 'chrome' pages from an unprivileged 'about:' page, which could lead to unauthorized access; and a window spoofing vulnerability was reported when a blank 'chrom' canvas is obtained by opening a window from a reference to a closed window, which could let a remote malicious user conduct phishing type attacks.<br>Firefox<br>Mozilla Browser<br>RedHat<br>Ubuntu<br>Mandriva<br>Fedora<br>Slackware<br>SGI<br>Conectiva<br>Gentoo<br>SUSE<br>Fedora<br>Debian<br>TurboLinux<br>Mandriva<br>Ubuntu<br>Netscape<br>Debian<br>Debian<br>**FedoraLegacy**<br>Currently we are not aware of any exploits for these vulnerabilities. | CVE-2005-2703<br>CVE-2005-2704<br>CVE-2005-2705<br>CVE-2005-2706<br>CVE-2005-2707 | 3.3<br>(CVE-2005-2703)<br>3.3<br>(CVE-2005-2704)<br>7<br>(CVE-2005-2705)<br>4.7<br>(CVE-2005-2706)<br>3.3<br>(CVE-2005-2707) | Advisory, RHSA-2005:789-11, September 22, 2005<br>Ubuntu Security Notices, USN-186-1 & 186-2, September 23 & 25, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:169 & 170, September 26, 2005<br>Fedora Update Notifications, FEDORA-2005-926-934, September 26, 2005<br>Slackware Security Advisory, SSA:2005-269-01, September 26, 2005<br>SGI Security Advisory, 20050903-02-U, September 28, 2005<br>Conectiva Linux Announcement, CLSA-2005:1017, September 28, 2005<br>Gentoo Linux Security Advisory [UPDATE], September 29, 2005<br>SUSE Security Announcement, SUSE-SA:2005:058, September 30, 2005<br>Fedora Update Notifications, FEDORA-2005-962 & 963, September 30, 2005<br>Debian Security Advisory, DSA 838-1, October 2, 2005<br>Turbolinux Security Advisory, TLSA-2005-93, October 3, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:174, October 6, 2005<br>Ubuntu Security Notice, USN-200-1, October 11, 2005<br>Security Focus, Bugtraq ID: 14916, October 19, 2005<br>Debian Security Advisories, DSA 866-1 & 868-1, October 20, 2005<br>**Fedora Legacy Update Advisory, FLSA:168375, January 9, 2006** |
| Multiple Vendors<br>Netscape Browser 8.0.3.3;<br>Mozilla Firefox 1.0-1.0.6, Mozilla Browser 1.7-1.7.11 | A remote Denial of Service vulnerability has been reported when a malicious user creates a Proxy Auto-Config (PAC) script that contains a specially crafted eval() statement.<br>Firefox<br>Mozilla Browser<br>**FedoraLegacy**<br>There is no exploit code required. | Multiple Browser Proxy Auto-Config Scripts Remote Denial of Service<br>CVE-2005-3089 | 1.9 | Security Tracker Alert ID: 1014949, September 21, 2005<br>**Fedora Legacy Update Advisory, FLSA:168375, January 9, 2006** |

| | | | | |
|---|---|---|---|---|
| Multiple Vendors<br>University of Kansas Lynx 2.8.5 & prior | A vulnerability has been reported in the 'lynxcgi:' URI handler, which could let a remote malicious user execute arbitrary commands.<br>Upgrades available<br>RedHat<br>Mandriva<br>Gentoo<br>Trustix<br>SGI<br>OpenPKG<br>SCO<br>FedoraLegacy<br>**SCO**<br>There is no exploit code required. | Lynx URI Handlers Arbitrary Command Execution<br>CVE-2005-2929 | 8.5 | Security Tracker Alert ID: 1015195, November 11, 2005<br>RedHat Security Advisory, RHSA-2005:839-3, November 11, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:211, November 12, 2005<br>Gentoo Linux Security Advisory, GLSA 200511-09, November 13, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0066, November 22, 2005<br>SGI Security Advisory, 20051101-01-U, November 29, 2005<br>OpenPKG Security Advisory, OpenPKG-SA-2005.026, December 3, 2005<br>SCO Security Advisory, SCOSA-2005.55, December 14, 2005<br>Fedora Legacy Update Advisory, FLSA:152832, December 17, 2005<br>**SCO Security Advisory, SCOSA-2006.7, January 10, 2006** |
| Multiple Vendors<br>MandrakeSoft Linux Mandrake 2006.0 x86_64, 2006.0, 10.2 x86_64, 10.2; Gentoo Linux; Ethereal Group Ethereal 0.10.1-0.10.13, 0.9-0.9.16, 0.8.19, 0.8.18, 0.8.13-0.8.15, 0.8.5, 0.8, 0.7.7 | A vulnerability has been reported in Ethereal, IRC Protocol Dissector, that could let remote malicious users cause a Denial of Service.<br>Mandriva<br>Gentoo<br>SUSE<br>Conectiva<br>**Fedora**<br>**RedHat**<br>Currently we are not aware of any exploits for this vulnerability. | Ethereal Denial of Service<br>CVE-2005-3313 | 3.3 | Mandriva Linux Security Advisory, MDKSA-2005:193-1, October 26, 2005<br>Gentoo Linux Security Advisor, GLSA 200510-25, October 30, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005<br>Conectiva Security Announce-ment, CLSA-2005:1043, November 8, 2005<br>**Fedora Update Notification FEDORA-2005-000, January 5, 2006**<br>**RedHat Security Advisory, RHSA-2006:0156-6, January 11, 2006** |

| | | | | |
|---|---|---|---|---|
| Multiple Vendors<br>PostNuke Development Team PostNuke 0.761; moodle 1.5.3; Mantis 1.0.0RC4, 0.19.4; Cacti 0.8.6 g; ADOdb 4.68, 4.66 | Several vulnerabilities have been reported: an SQL injection vulnerability was reported in the 'server.php' test script, which could let a remote malicious user execute arbitrary SQL code and PHP script code; and a vulnerability was reported in the 'tests/tmssql.php' text script, which could let a remote malicious user call an arbitrary PHP function.<br>Adodb<br>Cacti<br>Moodle<br>PostNuke<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | ADOdb Insecure Test Scripts<br>CVE-2006-0146<br>CVE-2006-0147 | 7<br>(CVE-2006-0146)<br>7<br>(CVE-2006-1047) | Secunia Advisory: SA17418, January 9, 2006 |
| Multiple Vendors<br>RedHat Fedora Core4, Core3; Ethereal Group Ethereal 0.10 -0.10.12, 0.9-0.9.16, 0.8.19, 0.8.18 | Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the ISAKMP, FC-FCS, RSVP, and ISIS LSP dissectors; a remote Denial of Service vulnerability was reported in the IrDA dissector; a buffer overflow vulnerability was reported in the SLIMP3, AgentX, and SRVLOC dissectors, which could let a remote malicious user execute arbitrary code; a remote Denial of Service vulnerability was reported in the BER dissector; a remote Denial of Service vulnerability was reported in the SigComp UDVM dissector; a remote Denial of service vulnerability was reported due to a null pointer dereference in the SCSI, sFlow, and RTnet dissectors; a vulnerability was reported because a remote malicious user can trigger a divide by zero error in the X11 dissector; a vulnerability was reported because a remote malicious user can cause an invalid pointer to be freed in the WSP dissector; a remote Denial of Service vulnerability was reported if the 'Dissect unknown RPC program numbers' option is enabled (not the default setting); and a remote Denial of Service vulnerability was reported if SMB transaction payload reassembly is enabled (not the default setting).<br>Upgrades available<br>Fedora:<br>RedHat<br>Mandriva<br>Avaya<br>Gentoo<br>SUSE<br>SGI<br>**FedoraLegacy**<br>An exploit script has been published. | Ethereal Multiple Protocol Dissector Vulnerabilities<br>CVE-2005-3184<br>CVE-2005-3241<br>CVE-2005-3242<br>CVE-2005-3243<br>CVE-2005-3244<br>CVE-2005-3245<br>CVE-2005-3246<br>CVE-2005-3247<br>CVE-2005-3248<br>CVE-2005-3249 | 10<br>(CVE-2005-3184)<br>3.3<br>(CVE-2005-3241)<br>3.3<br>(CVE-2005-3242)<br>7<br>(CVE-2005-3243)<br>3.3<br>(CVE-2005-3244)<br>3.3<br>CVE-2005-3245)<br>3.3<br>(CVE-2005-3246)<br>3.3<br>(CVE-2005-3247)<br>3.3<br>(CVE-2005-3248)<br>6.7<br>(CVE-2005-3249) | Ethereal Security Advisory, enpa-sa-00021, October 19, 2005<br>Fedora Update Notifications, FEDORA-2005-1008 & 1011, October 20, 2005<br>RedHat Security Advisory, RHSA-2005:809-6, October 25, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:193, October 25, 2005<br>Avaya Security Advisory, ASA-2005-227, October 28, 2005<br>Gentoo Linux Security Advisory, GLSA 200510-25, October 30, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:193-2, October 31, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005<br>SGI Security Advisory, 20051101-01-U, November 29, 2005<br>**Fedora Legacy Update Advisory, FLSA:152922, January 9, 2006** |
| Multiple Vendors<br>Ubuntu Linux 5.10 powerpc, i386, amd64; Blender 2.40 alpha, 2.39, 2.37 a, 2.37, 2.30-2.35, 2.25 -2.28, 2.0 4 | A buffer overflow vulnerability has been reported in 'get_bhead()' when parsing '.blend' files, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.<br>Ubuntu<br>A Proof of Concept exploit has been published. | Blender Buffer Overflow<br>CVE-2005-4470 | 8 | Ubuntu Security Notice, USN-238-2, January 06, 2006 |
| Multiple Vendors<br>University of Kansas Lynx 2.8.6 dev.1-dev.13, 2.8.5 dev.8, 2.8.5 dev.2-dev.5, 2.8.5, 2.8.4 rel.1, 2.8.4, 2.8.3 rel.1, 2.8.3 pre.5, 2.8.3 dev2x, 2.8.3 dev.22, 2.8.3, 2.8.2 rel.1, 2.8.1, 2.8, 2.7;<br>RedHat Enterprise | A buffer overflow vulnerability has been reported in the 'HTrjis()' function when handling NNTP article headers, which could let a remote malicious user execute arbitrary code.<br>University of Kansas Lynx<br>Gentoo<br>Ubuntu<br>RedHat<br>Fedora | Lynx 'HTrjis()' NNTP Remote Buffer Overflow<br>CVE-2005-3120 | 7 | Gentoo Linux Security Advisory, GLSA 200510-15, October 17, 2005<br>Ubuntu Security Notice, USN-206-1, October 17, 2005<br>RedHat Security Advisory, RHSA-2005:803-4, October 17, 2005 |

| | | | | |
|---|---|---|---|---|
| Linux WS 4, WS 3, 2.1, ES 4, ES 3, ES 2.1, AS 4, AS 3, AS 2.1,<br>RedHat Desktop 4.0, 3.0,<br>RedHat Advanced Workstation for the Itanium Processor 2.1 IA64 | Mandriva<br>Conectiva<br>Trustix<br>SGI<br>Mandriva<br>Debian<br>Debian<br>Ubuntu<br>(Note: Ubuntu advisory USN-206-1 was previously released to address this vulnerability, however, the fixes contained an error that caused lynx to crash.)<br>SUSE<br>Slackware<br>SCO<br>OpenPKG<br>FedoraLegacy<br>**SCO**<br>A Proof of Concept Denial of Service exploit script has been published. | | | Fedora Update Notifications, FEDORA-2005-993 & 994, October 17, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:186, October 18, 2005<br>Conectiva Linux Announcement, CLSA-2005:1037, October 19, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0059, October 21, 2005<br>SGI Security Advisory, 20051003-01-U, October 26, 2005<br>Mandriva Linux Security Advisory, MDKSA-2005:186-1, October 26, 2005<br>Debian Security Advisories, DSA 874-1 & 876-1, October 27, 2005<br>Ubuntu Security Notice, USN-206-2, October 29, 2005<br>SUSE Security Summary Report, SUSE-SR:2005:025, November 4, 2005<br>Slackware Security Advisory, SSA:2005-310-03, November 7, 2005<br>SCO Security Advisory, SCOSA-2005.47, November 8, 2005<br>OpenPKG Security Advisory, OpenPKG-SA-2005.026, December 3, 2005<br>Fedora Legacy Update Advisory, FLSA:152832, December 17, 2005<br>**SCO Security Advisory, SCOSA-2006.7, January 10, 2006** |
| MyPhPim<br>MyPhPim 01.05 | Multiple vulnerabilities have been reported: a file upload vulnerability was reported in the 'addresses.php3' script, which could let a remote malicious user execute arbitrary code; an SQL injection vulnerability was reported in 'calendar.php3' due to insufficient sanitization of the 'cal_id' parameter and in the password field when logging, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the description field when creating a new todo, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, Proof of Concept exploits have been published. | MyPHPim Multiple Vulnerabilities<br>CVE-2006-0167<br>CVE-2006-0168<br>CVE-2006-0169 | Not available | Secunia Advisory: SA18399, January 11, 2006 |
| Navboard<br>Navboard V17beta2, V16 | A vulnerability has been reported due to insufficient sanitization of input received via certain BBcode tags, which could let a remote malicious user execute arbitrary JavaScript code. | NavBoard BBcode Script Insertion<br>CVE-2006-0140 | 2.3 | Security Focus, Bugtraq ID: 16165, January 7, 2006 |

| | | | | |
|---|---|---|---|---|
| | No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0019.txt, have been published. | | | |
| OnePlug Solutions<br>OnePlug CMS | SQL injection vulnerabilities have been reported due to insufficient sanitization of unspecified input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, Proof of Concept exploits have been published. | OnePlug CMS SQL Injection<br>CVE-2006-0115 | 7 | Secunia Advisory: SA18325, January 6, 2006 |
| OpenSSH<br>OpenSSH 4.1, 4.0, p1 | Several vulnerabilities have been reported: a vulnerability was reported due to an error when handling dynamic port forwarding when no listen address is specified, which could let a remote malicious user cause "GatewayPorts" to be incorrectly activated; and a vulnerability was reported due to an error when handling GSSAPI credential delegation, which could let a remote malicious user be delegated with GSSAPI credentials.<br>OpenBSD<br>Fedora<br>Trustix<br>Slackware<br>Fedora<br>RedHat<br>Mandriva<br>Ubuntu<br>Conectiva<br>HP<br>There is no exploit code required. | OpenSSH DynamicForward Inadvertent GatewayPorts Activation & GSSAPI Credentials<br>CVE-2005-2797<br>CVE-2005-2798 | 3.3 (CVE-2005-2797)<br>3.3 (CVE-2005-2798) | Secunia Advisory: SA16686, September 2, 2005<br>Fedora Update Notification, FEDORA-2005-858, September 7, 2005<br>Trustix Secure Linux Security Advisory, TSLSA-2005-0047, September 9, 2005<br>Slackware Security Advisory, SSA:2005-251-03, September 9, 2005<br>Fedora Update Notification, FEDORA-2005-860, September 12, 2005<br>RedHat Security Advisory, RHSA-2005:527-16, October 5, 2005<br>Mandriva Linux Security Update Advisory, MDKSA-2005:172, October 6, 2005<br>Ubuntu Security Notice, USN-209-1, October 17, 2005<br>Conectiva Linux Announcement, CLSA-2005:1039, October 19, 2005<br>**Security Focus, Bugtraq ID: 14729, January 10, 2006** |
| Orjinweb E-commerce<br>Orjinweb E-commerce | A file include vulnerability has been reported in 'index.php' due to insufficient sanitization, which could let a remote malicious user execute arbitrary PHP code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit, orjinweb.txt, has been published. | Orjinweb Remote File Include<br>CVE-2006-0171 | Not available | Security Focus, Bugtraq ID: 16199, January 10, 2006 |
| PHP-Nuke<br>PHP-Nuke EV 7.7 | An SQL injection vulnerability has been reported in the search module due to insufficient sanitization of the 'query' variable before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | PHPNuke EV Search Module SQL Injection<br>CVE-2006-0163 | 7 | Security Focus, Bugtraq ID: 16186, January 9, 2006 |
| PHP-Nuke<br>PHP-Nuke Pool Module, News Module | An HTML injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in dynamically generated content, which could let a remote malicious user execute arbitrary HTML and script code. | PHPNuke Multiple Modules HTML Injection<br>CVE-2006-0185 | 2.3 | Security Focus, Bugtraq ID: 16192, January 10, 2006 |

| | | | | |
|---|---|---|---|---|
| | No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | | | |
| Ralph Capper<br>TinyPHPForum 3.6 | Several vulnerabilities have been reported: a vulnerability was reported due to insufficient verification of input passed to the URL of a link when posting a message, which could let a remote malicious user execute arbitrary JavaScript; a vulnerability was reported in the 'users' directory because user credentials are stored insecurely, which could let a remote malicious user obtain sensitive information; and a Directory Traversal vulnerability was reported in 'profile.php' due to insufficient sanitization of the 'uname' parameter when viewing a profile, which could let a remote malicious user obtain sensitive information.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0014.txt, have been published. | TinyPHPForum Information Disclosure & Cross-Site Scripting<br>CVE-2006-0102<br>CVE-2006-0103<br>CVE-2006-0104 | 2.3<br>(CVE-2006-0102)<br>2.3<br>(CVE-2006-0103)<br>2.3<br>(CVE-2006-0104) | Security Tracker Alert ID: 1015436, January 5, 2005 |
| Reamday Enterprises<br>Magic News Plus 1.0.3 | A vulnerability has been reported due to insufficient verification of user-supplied input, which could let a remote malicious user change the administrator password.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, Proof of Concept exploit scripts, MagicNewsPlus-pw-change.pl and cijfer-mnxpl.pl.txt, have been published. | Magic News Plus Administrator Password Change<br>CVE-2006-0157 | 2.3 | Security Focus, Bugtraq ID: 16182, January 9, 2006 |
| Research In Motion<br>Blackberry Enterprise Server for Novell Groupwise 4.0, SP1 & SP2, Enterprise Server for Exchange 4.0, SP1 & SP2, Enterprise Server for Domino 4.0, SP1 & SP2 | A remote Denial of Service vulnerability has been reported when handling a malformed PNG attachment.<br>Update available<br>Currently we are not aware of any exploits for this vulnerability. | Blackberry Enterprise Server Attachment Service PNG Attachment Remote Denial of Service<br>CVE-2005-2344 | 2.3 | Secunia Advisory: SA18393,<br>US-CERT, VU#646976 |
| TheWeb Forum<br>TheWebForum 1.2.1 | Several input validation vulnerabilities have been reported: an SQL injection vulnerability was reported due to insufficient sanitization of the 'username' parameter in 'login.php' before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of the'register.php' script, which could let a remote malicious user execute arbitrary HTML and script code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, exploit details, EV0017.txt, have been published. | TheWebForum SQL Injection & Cross-Site Scripting<br>CVE-2006-0134<br>CVE-2006-0135 | 2.3<br>(CVE-2006-0134)<br>7<br>(CVE-2006-0135) | New eVuln Advisory, January 6, 2006 |
| Venom Board<br>Venom Board 1.22 | SQL injection vulnerabilities have been reported due to insufficient sanitization of the '$parent,' '$root,' and '$topic_id' variables before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code.<br>No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit, EV0021.txt, has been published. | Venom Board Post.PHP3 Multiple SQL Injection<br>CVE-2006-0160 | 7 | eVuln Advisory, January 9, 2006 |
| VMWare, Inc.<br>VMWare ESX Server 2.5.2, 2.5, 2.1-2.1.2, 2.0.1 build 6403, 2.0.1, 2.0 build 5257, 2.0 | A vulnerability has been reported in the VMware Management Interface due to an unspecified error, which could let a remote malicious user execute arbitrary code.<br>Patches available<br>Gentoo<br>Currently we are not aware of any exploits for this vulnerability. | VMware ESX Server Management Interface Remote Arbitrary Code Execution<br>CVE-2005-4583 | 2.3 | Security Tracker Alert ID: 1015422, December 29, 2005<br>**Gentoo Linux Security Advisory, GLSA 200601-04, January 7, 2006** |
| Xoops<br>Xoops Pool Module | An HTML injection vulnerability has been reported in the IMG tag due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. | Xoops Pool Module HTML Injection | Not available | Security Focus, Bugtraq ID: 16189, January 9, 2006 |

| | | |
|---|---|---|
| | No workaround or patch available at time of publishing.<br>There is no exploit code required; however, a Proof of Concept exploit has been published. | |

[back to top]

# Wireless Trends & Vulnerabilities

This section contains wireless vulnerabilities, articles, and malicious code that has been identified during the current reporting period.

- Blackberry Enterprise Server Attachment Service PNG Attachment Remote Denial of Service: A remote Denial of Service vulnerability has been reported when handling malformed PNG attachments.
- British Parliament members demand Wi-Fi access: Wireless Internet access should be installed in parts of the Houses of Parliament to give its members access to information on the move. According to a report by the U.K. House of Commons Administration Committee, they are calling for secure wireless access after it found that some new members of Parliament struggled to work before they were given office space.
- Wireless Spending To Exceed Wireline In 2006: Study: According to a study by market research firm, In-Stat, enterprises will spend more for wireless voice service than on wireline in 2006. In addition, the study found that wireless data service will start growing quickly, with an average growth rate of 18 percent a year through 2009.

[back to top]

# General Trends

This section contains brief summaries and links to articles which discuss or present information pertinent to the cyber security community.

- Security flaws on the rise, questions remain: The number of publicly reported vulnerabilities jumped in 2005. This number was boosted by easy-to-find bugs in Web applications. A survey of four major vulnerability databases found that the number of flaws counted by each in the past five years differed significantly. However, three of the four databases exhibited a relative plateau in the number of flaws publicly disclosed in 2002 through 2004. And, every database saw a significant increase in their count of the flaws disclosed in 2005. Recent numbers produced by the U.S. Computer Emergency Readiness Team (US-CERT) revealed some of the problems with refined vulnerability sources. Managed by the CERT Coordination Center, the US-CERT's security bulletins outline security issues but are updated each week. In a year end list published last week, the US-CERT announced that 5,198 vulnerabilities had been reported in 2005.
- Your IM Buddy, Or A Hacker? It's Getting Harder To Tell: Instant-messaging security vendors FaceTime Communications Inc. and IMlogic Inc. reported that malware delivered over instant-message clients skyrocketed in recent months. There has been more than a 20-fold increase in the number of reported IM worm and virus variants since 2004.
- Popular certifications don't ensure security: According to a survey from the SANS Institute, many popular information technology security certifications don't improve holders' ability to ensure computer systems' security, according to a new survey from the SANS Institute, a training and education organization for security professionals.

[back to top]

# Viruses/Trojans

### Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

| Rank | Common Name | Type of Code | Trend | Date | Description |
|---|---|---|---|---|---|
| 1 | Netsky-P | Win32 Worm | Stable | March 2004 | A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders. |
| 2 | Mytob-GH | Win32 Worm | Stable | November 2005 | A variant of the mass-mailing worm that disables security related programs and allows other to access the infected system. This version sends itself to email addresses harvested from the system, forging the sender’s address. |
| 3 | Netsky-D | Win32 Worm | Stable | March 2004 | A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only. |
| 4 | Zafi-B | Win32 Worm | Stable | June 2004 | A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names. |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| 5 | Sober-Z | Win32 Worm | Stable | December 2005 | This worm travels as an email attachment, forging the senders address, harvesting addresses from infected machines, and using its own mail engine. It further download code from the internet, installs into the registry, and reduces overall system security. |
| 6 | Lovgate.w | Win32 Worm | Stable | April 2004 | A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network. |
| 7 | Mytob.C | Win32 Worm | Stable | March 2004 | A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files. |
| 8 | Zafi-D | Win32 Worm | Stable | December 2004 | A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer. |
| 9 | Mytob-BE | Win32 Worm | Stable | June 2005 | A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling anti virus, and modifying data. |
| 10 | Mytob-AS | Win32 Worm | Stable | June 2005 | A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine. |

Table updated January 11, 2006

[back to top]

**Last updated**